
TODO LO QUE NADIE HA OSADO DECIRTE ANTES
HACKER
JOURNAL
n. 10
www.hacker-journal.com
BIMENSUAL AÑO 3 - 2005
BLUE BUGGING
HACKMACHINE
2€
SIN PUBLICIDAD
SÓLO INFORMACIÓN Y ARTÍCULOS
PROGRAMAR COMO SHAKESPEARE
Emmanuel Goldstein:
PROFESOR HACKER
00010
8 413042 435235
Secuestros on-line:
ataques a los
CASINOS



Año 3 - N. 10 - 2005

Director Responsable:
Luca Sprea

Los chicos de la redacción europea:
Federico Cociancich, Amadeu Brugués, Eric Sala, Infoambiente, Gualtiero Tronconi, Eduardo Bracaglia, Gregorio Peron, Contents by MDR

Colaboradores: Bismark, Fabio Benedetti, Guillermo Cancelli, Gaia, Nicolás A., Lele, Roberto "decOder" Enea, >>>----Robin---->, Lidia, 3dO, Eric Sala, Mònica Batalla, Anna Riera

Maquetación: Estudi Digital, S.L.

Diseño gráfico: Dopla Graphic S.r.l.
info@dopla.com

Redacción
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printed in Italy

Difusión: Paul-Luc PEREZ

Distribución
SGEL - Avda Valdelaparra 29
Poligono Industrial De Alcobendas
Madrid - Spain

Publicación bimensual registrada el 14/2/03 con el número MI2003C/001404

hack'er (hãk'ər)

"Persona que se divierte explorando los detalles de los sistemas de programación y expandiendo sus capacidades, a diferencia de muchos usuarios que prefieren aprender solamente lo mínimo necesario."

LECCIONES PRÁCTICAS

La variedad ha sido la pretensión básica en la preparación del número de Hacker Journal que tenéis entre manos. Abrimos con una lección en directo de ingeniería social, para que nos ayude a tomar conciencia de que por mucho que nos esforcemos en asegurar nuestras instalaciones informáticas, hay que seguir formando e informando a los usuarios para mantener la información y la privacidad a salvo. A continuación, analizamos diversos ataques con rehenes virtuales, los sitios web, que no siempre acaban bien, pero sí a veces. Y acto seguido, encontraréis el cuaderno de bitácora del récord de conexión wi-fi conseguido en medio del desierto. Para los amantes de las grandes antenas, esto va a ser un festival...

Después nos ponemos el mono de trabajo y nos dedicamos a lo nuestro: trastear el hardware siempre tiene algo de fascinante, tal vez por el factor riesgo. Os mostramos cómo se ha conseguido batir el récord, en esta ocasión de overclocking de un Pentium. Y también pasamos revista al software, para desactivar los programas de censorware que, en tantas ocasiones, han resultado ser filtros de sitios con intención de favorecer a determinadas marcas en lugar de lo que prometen ser: unas niñeras virtuales angelicales.

Encontraréis también el retrato robot de Emmanuel Goldstein, un personaje controvertido donde los haya. Nunca está de más conocer trucos y secretos de Windows, de modo que en un par de páginas os exponemos algunos de los más interesantes. Para quienes tengan aspiraciones literarias, también podréis dedicaros a la literatura mientras programáis, siempre que os guste la obra teatral de Shakespeare. En cambio, si lo que queréis es usar el soldador, os enseñamos a montaros vuestra propia linterna privada para el portátil (que también será útil en un equipo de sobremesa) mediante una conexión USB. Tras hablar de los grandes números primos, presentamos las debilidades de los teléfonos Bluetooth. Y nos despedimos con una breve pero intensa historia de la informática personal. ¡Que lo disfrutéis!

redaccion@hacker-journal.com

UNA REVISTA PARA TODOS







El mundo hacker se compone de algunas cosas simples y otras complicadas. Hay curiosos, lectores sin experiencia y expertos para los cuales el ordenador no tiene secretos. Cada artículo de Hacker Journal está marcado con una clave para cada nivel: NEWBIE (para quien comienza), MIDHACKING (para quien ya está dentro) y HARDHACKING (para quien no existen los secretos).

SUMARIO



SITIO WEB

Como en cada número de Hacker Journal, os recordamos que tenéis a vuestra disposición el sitio web de la revista, www.hacker-journal.com, para seguir leyendo y aprendiendo sobre el Hacking. Recordad también que disponéis de los foros donde podéis exponer dudas y preguntas, observaciones, etcétera. Todos los visitantes del sitio web colaborarán en hallar respuesta a todas las preguntas. ¡Entre todos lo conseguiremos!

Visita nuestro sitio web:
www.hacker-journal.com

CODIGO DE LA SECRET ZONE
user: secreto10
password: decimal10

User:
2€ SIN PUBLICI... SÓLO INFORMA... Y ARTÍCUL...

15 Dic 2004 - 01:14 PM

HOME | NEWS | REVIEWS | FORUMS | GALLERY

Newsletter
email address
Enviar

Try2hack
Enter here

Main Menu
- Home

Servicios
- Descargas
- FAQ
- Lista de miembros
- News
- Recomienda hjes
- Reviews
- Buscar
- Sesiones
- Estadísticas
- Enviar un artículo
- Topics
- Top List
- Enlaces
- Forum [new]

Número 9 - Hacker Journal

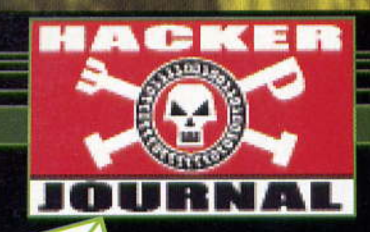
¡En tu kiosco!
Sumario:

- Comparativa: el mejor antimalware
- Solsticio de invierno: Diálogo con el hacker socrático
- Libertad de XOR: ¿sigue vigente el copyright tras modificación digital?
- Archivos invisibles en Windows: dónde están, qué hacen, por qué son invisibles y cómo acceder a ellos
- Wine: Windows en Linux
- Dirección enmascarada
- Máximo secreto con KGB
- Del lenguaje natural al C y viceversa

Número 6 - Hackers Magazine

¡En tu kiosco!
En este número encontrarás:

- Cómo revelar los passwords
- Los mejores cortafuegos para proteger la Red
- Hacer invisibles archivos carpetas
- Folder Lock: protege nuestros datos más personales
- CLAM: un antivirus gratuito y eficaz





mailto:
redaccion@hacker-journal.com

PROFUNDAS REFLEXIONES

Apreciados amigos de Hacker Journal: ante todo felicitaros por la revista, que aunque tiene montones de cosas a mejorar me parece muy buena y tal como está el panorama es de agredecer vuestra presencia. Os mando un texto que me llegó hace tiempo en un mensaje. Es un poco largo, pero como programador me sigue pareciendo tan interesante como el primer día. Espero que lo publiquéis. Gracias.

ENTREVISTA A BJARNE STROUSTRUP, CREADOR DEL C++

El 1 de Enero de 1998, Bjarne Stroustrup dio una entrevista a la revista de informática del IEEE. Al finalizar la entrevista, el entrevistador consiguió más de lo que había pactado en un principio, y consecuentemente, el editor decidió suprimir los contenidos 'por el bien de la industria'. Pero como suele suceder, la información se filtró...

Aquí esta una completa transcripción de lo que se dijo, no editado, no ensayado, es decir que no es como las entrevistas planeadas...

Entrevistador: Bien, hace unos pocos años que cambio el mundo del diseño de software, ¿como se siente mirando atrás?

BS: En este momento estaba pensando en aquellos días, justo antes de que llegases. ¿Los recuerdas? Todo el mundo escribía en C y el problema era que eran demasiado buenos... Las Universidades eran demasiado buenas enseñándolo también. Se estaban graduando programadores competentes a una velocidad de vértigo. Esa era la causa del problema.

Entrevistador: ¿Problema?

BS: Si, problema. ¿Recuerdas cuando todos programaban en Cobol?

Entrevistador: Desde luego. Yo también lo hice.

BS: Bien, al principio, esos tipos eran como semidioses. Sus salarios eran altos, y eran tratados como la realeza...

Entrevistador: Aquellos fueron buenos tiempos, ¿eh?

BS: Exacto. Pero, ¿que pasó? IBM se cansó de ello, e invirtió millones en entrenar a programadores, hasta el punto que podías comprar una docena por medio dólar...

Entrevistador: Eso es por lo que me fui. Los salarios bajaron en un año hasta el punto de que el trabajo de periodista está mejor pagado.

BS: Exactamente. Bien, lo mismo pasó con los programadores de C...

Entrevistador: Ya veo, pero ¿adonde quiere llegar?

BS: Bien, un día, mientras estaba sentado en la oficina, pensaba en este pequeño esquema, que podría inclinar la balanza un poquito. Pensé '¿Que ocurriría si existiese un lenguaje tan complicado, tan difícil de aprender, que nadie fuese capaz de inundar el mercado de programadores?' Empecé cogiendo varias ideas del X10, ya sabes, XWindows. Es una auténtica pesadilla de sistemas gráficos, que solo se ejecutaba en aquellas cosas Sun 3/60...tenía todos los ingredientes que yo buscaba. Una sintaxis ridículamente compleja, funciones oscuras y estructuras pseudo-OO. Incluso ahora nadie escribe en código nativo para las X-Windows. Motif es el único camino a seguir si quieres mantener la cordura.

Entrevistador: ¿Está bromeando?

BS: Ni un pelo. De hecho, existe otro problema... Unix está escrito en C, lo que significa que un programador en C puede convertirse fácilmente en un programador de sistemas. ¿Recuerdas el dinero que un programador de sistemas solía conseguir?

Entrevistador: Puede apostar por ello. Es lo que solía hacer yo...

BS: OK, por lo tanto, este nuevo lenguaje tenía que divorciarse por si mismo de Unix, ocultando las llamadas al sistema. Esto podría permitir a tipos que solo conocían el DOS ganarse la vida decentemente...

Entrevistador: No me puedo creer que haya dicho eso...

BS: Bueno, ha llovido mucho desde entonces. Ahora creo que la mayoría de la gente se habrá figurado que C++ es una perdida de tiempo, pero debo decir que han tardado más en darse cuenta de lo que pensaba.

Entrevistador: ¿Entonces, que hizo exactamente?

BS: Se suponía que tenía que ser una broma, nunca pense que la gente se tomase el libro en serio. Cualquiera con dos dedos de frente puede ver que la programación orientada a objetos es anti intuitiva, ilógica e ineficiente...

Entrevistador: ¡¿Que?!

Nuestra enhorabuena a: Roberto Torres y Lander Cayetano por su respuesta al cyberenigma del número anterior de HJ.

BS: Y como el código reutilizable... ¿cuando has oído de una compañía que reutilice su código?

Entrevistador: Bien, nunca, pero...

BS: Entonces estas de acuerdo. Recuerda, algunos lo intentaron al principio. Había esa compañía de Oregon, creo que se llamaba Mentor Graphics, que reventó intentando reescribir todo en C++ en el 90 o 91. Lo siento realmente por ellos, pero pense que los demás aprenderían de sus errores.

Entrevistador: Obviamente no lo hicieron, ¿verdad?

BS: Ni lo mas mínimo. El problema es que la mayoría de las empresas se callaron sus mayores disparates, y explicar 30 millones de dólares de perdidas a los accionistas podría haber sido difícil... Démosles el reconocimiento que merecen, finalmente consiguieron hacer que funcionase.

Entrevistador: ¿Lo hicieron? Bien eso demuestra que la POO funciona...

BS: Casi. El ejecutable era tan gigantesco que tardaba unos cinco minutos en cargar en una estación de trabajo de HP con 128 MB de RAM. Iba tan rápido como un triciclo. Creí que sería un escollo insalvable pero nadie se preocupó. SUN y HP estaban demasiado alegres de vender enormes y poderosas máquinas con gigantescos recursos para ejecutar programas triviales. Ya sabes, cuando hicimos nuestro primer compilador de C++, en AT&T, compilé el clásico 'Hello World', y no me podía creer el tamaño del ejecutable. 2.1 MB.

Entrevistador: ¡¿Que?!. Bueno, los compiladores han mejorado mucho desde entonces...

BS: ¿Lo han hecho? Inténtalo en la última versión de g++, la diferencia no será mayor que medio mega. Además, existen multitud de ejemplos actuales en todo el mundo. British Telecom tuvo un desastre mayor en sus manos, pero, afortunadamente, se deshicieron de ello y comenzaron de nuevo. Tuvieron más suerte que Australian Telecom. Ahora he oído que Siemens está construyendo un dinosaurio y se empiezan a preocupar porque los recursos hardware no hacen más que crecer para hacer funcionar e-

jecutables típicos. ¿No es una delicia la herencia múltiple?
Entrevistador: Bien, pero C++ es un lenguaje avanzado...
BS: ¿Realmente crees eso? Te has sentado alguna vez y te has puesto a trabajar en un proyecto C++? Esto es lo que sucede: Primero he puesto las suficientes trampas para asegurarme que solo los proyectos mas triviales funcionen a la primera. Coge la sobrecarga de operadores. Al final del proyecto casi todos los módulos lo tienen, normalmente los programadores sienten que deberían hacerlo así porque es como les enseñaron en sus cursos de aprendizaje. El mismo operador entonces significa cosas diferentes en cada módulo. Intenta poner unos cuantos juntos, cuando tengas unos cientos de módulos. Y para la ocultación de datos. Dios, a veces no puedo parar de reírme cuando oigo los problemas que algunas empresas han tenido al hacer a sus módulos comunicarse entre si. Creo que el término 'sinergético' fue especialmente creado para retorcer un cuchillo en las costillas del director de proyecto...
Entrevistador: Tengo que decir que me siento bastante pasmado por todo esto. ¿Dice que consiguió subir el salario de los programadores? Eso es inmoral.
BS: No del todo. Cada uno tiene su opción. Yo no esperaba que la cosa se me fuese tanto de las manos. De cualquier forma acerté. C++ se esta muriendo ahora, pero los programadores todavía conservan sus sueldos altos. Especialmente esos pobres diablos que tienen que mantener toda esta majadería. ¿Comprendes que es imposible mantener un gran módulo en C++ si no lo has escrito tu mismo?
Entrevistador: ¿Como?
BS: ¿Estás fuera de juego, verdad? ¿Recuerdas 'typedef'?
Entrevistador: Si, desde luego.
BS: ¿Recuerdas cuanto tiempo se perdía buscando a tientas en las cabeceras solo para darse cuenta de que 'RoofRaised' era un número de doble precisión? Bien, imagina el tiempo que te puedes tirar para encontrar todos los typedefs implícitos en todas las clases en un gran proyecto.
Entrevistador: ¿En que se basa para creer que ha tenido éxito?
BS: ¿Te acuerdas de la duración media de un proyecto en C?. Unos 6 meses. No mucho para que un tipo con una mujer e hijos pueda conseguir un nivel de vida decente. Coge el mismo proyecto, realízalo en C++ y que obtienes? Te lo diré. Uno o dos años. ¿No es grandioso? Mucha más seguridad laboral solo por un error de juicio. Y una cosa más. Las universidades no han estado enseñando C desde hace mucho tiempo, lo que produce un descenso del número de buenos programadores en C. Especialmente de los que saben acerca de la programación en sistemas Unix. ¿Cuantos tipos sabrían que hacer con un 'malloc', cuando han estado usando 'new' durante estos años y nunca se han preocupado de chequear el código de retorno?. De hecho la mayoría de los programadores en C++ pasan de los códigos que les devuelven las funciones. ¿Que paso con el '-1'? Al menos sabías que tenias un error, sin enredarte con 'throw', 'catch', 'try'...
Entrevistador: ¿Pero seguramente la herencia salve un montón de tiempo?
BS: ¿Lo hace? ¿Te has fijado en la diferencia entre un proyecto en C y el mismo en C++? La etapa en la que se desarrolla un plan en un proyecto en C++ es tres veces superior. Precisamente para asegurarse de que todo lo que deba heredarse, lo hace, lo que no, no. Y aun así sigue dando fallos. ¿Quien ha oído hablar de la pérdida de memoria en un programa en C? Ahora se ha creado una auténtica industria especializada en encontrarlas. Muchas empresas se rinden y sacan el producto, sabiendo que pierde como un colador, simplemente para reducir el gasto de buscar todas esas fugas de memoria.
Entrevistador: Hay herramientas...
BS: La mayoría escritas en C++.
Entrevistador: Si publicamos esto, probablemente le lincharan. ¿Se da cuenta?
BS: Lo dudo. Como dije, C++ esta en su fase descendente ahora y ninguna compañía en su sano juicio comenzaría un proyecto en C++ sin una prueba piloto. Eso debería convencerles de que es un camino al desastre. Si no lo hace, entonces se merecen todo lo que les pase. ¿Ya sabes?, yo intente convencer a Dennis Ritchie a reescribir Unix en C++...
Entrevistador: Oh Dios. ¿Que dijo?
BS: Afortunadamente tiene un buen sentido del humor. Creo que tanto él como Brian se figuraban lo que estaba haciendo en aquellos días, y nunca empezaron el proyecto. Me dijo que me ayudaría a escribir una versión en C++ de DOS, si estaba interesado...
Entrevistador: ¿Lo estaba?
BS: De hecho ya he escrito DOS en C++, te pasare una demo cuando pueda. Lo tengo ejecutándose en una Sparc 20 en la sala de ordenadores. Va como un cohete en 4 CPUs, y solo ocupa 70 megas de disco...
Entrevistador: ¿Como se comporta en un PC?
BS: Ahora estás bromeando. ¿No has visto Windows '95? Creo que es mi mayor éxito. Casi acaba con la partida antes de que estuviese preparado.
Entrevistador: Ya sabes, la idea de Unix++ me ha hecho pensar. Quizás haya alguien ahí fuera intentándolo.
BS: No después de leer esta entrevista.
Entrevistador: Lo siento, pero no nos vemos capaces de publicar esto.
BS: Pero es la historia del siglo. Solo quiero ser recordado por mis compañeros programadores, por lo que he hecho por ellos. ¿Sabes cuanto puede conseguir un programador de C++ hoy día?
Entrevistador: Lo último que oí fue algo como unos $70 - $80 la hora para uno realmente bueno...
BS: ¿Lo ves? Y se los gana a pulso. Seguir la pista de todo lo que he puesto en C++ no es fácil. Y como dije anteriormente, todo programador en C++ se siente impulsado por alguna promesa mística a usar todos los elementos del lenguaje en cada proyecto. Eso ciertamente me molesta a veces, aunque sirva a mi propósito original. Casi me ha acabado gustando el lenguaje tras todo este tiempo.
Entrevistador: ¿Quiere decir que no era así antes?
BS: Lo odiaba. Parece extraño, no estás de acuerdo? Pero cuando los beneficios del libro empezaron a llegar... bien, te haces una idea...
Entrevistador: Solo un minuto. ¿Que hay de las referencias?. Debe admitir que mejoro los punteros de C...
BS: Hmm. Siempre me he preguntado por eso. Originalmente creí que lo había hecho. Entonces, un día estaba discutiendo esto con un tipo que escribe en C++ desde el principio. Dijo que no podía recordar cuales de sus variables estaban o no referenciadas, por lo que siempre usaba punteros. Dijo que el pequeño asterisco se lo recordaba.
Entrevistador: Bien, llegados a este punto suelo decir 'muchas gracias' pero hoy no parece muy adecuado.
BS: Prométeme que publicaras esto. Mi conciencia esta dando lo mejor de mi mismo estos días.
Entrevistador: Se lo haré saber, pero creo que se lo que dirá mi editor...
BS: ¿Quien se lo creería de todas formas?... ¿De todos modos, puedes enviarme una copia de la cinta.?
Entrevistador: Descuide, lo haré

COSME++

¡HOT!

BITTORRENT, 35% DEL TRÁFICO DE INTERNET

Según un artículo de Reuters, BitTorrent suma un 35% de todo el tráfico en Internet, más que el tráfico combinado del resto de programas P2P, y por supuesto dejando muy atrás el tráfico generado por las páginas web.

Además, en el artículo se detalla cómo BitTorrent no está en el objetivo de las empresas que demandan a los usuarios que comparten archivos. Sin embargo, a medida que su popularidad vaya en aumento es posible que asociaciones como la MPAA (Motion Picture Association of America) empiecen a vigilar a los usuarios de dicha red.

Según John Malcolm, director de operaciones mundiales de la MPAA, en declaraciones a la agencia Reuters: "Somos conscientes del volumen de material con copyright que se intercambia mediante BitTorrent. Es un sistema de intercambio muy efectivo para archivos grandes, y está siendo utilizado de forma abusiva por mucha gente. Estamos estudiando medidas, como solemos hacer con todas las nuevas tecnologías que se utilizan para cometer robos."

BitTorrent se ha convertido también en una forma estandar de descargar las distribuciones de linux. El éxito de este sistema operativo, lógicamente, carga el tráfico de la red con la disponibilidad gratuita de muchas de las distribuciones disponibles.

¡DENUNCIADME!

Con esta concisa elocuencia desafia Jon DVD (Jon Lech), el noruego que quebró el sistema de encriptación de DVD, a la todapoderosa Microsoft. Este joven ha colgado en su sitio personal un codigo que pretende universalizar el formato Windows Media 9.

Hasta ahora, los archivos Windows Media tan solo eran visibles en Windows y Mac OS. Una situación que Johansen considera injusta y a la que se enfrenta en su homepage con el provocador lema de "Denunciadme".

Jon ha colgado en su página un programa de Linux que permite que los archivos de Windows Media 9 puedan verse en el sistema universal VLC.

MSN SPACES



Un weblog es un sitio web donde se recopilan cronológicamente mensajes de uno o varios autores, sobre una temática en particular o a modo de diario personal, siempre conservando el autor la libertad de dejar publicado lo que crea pertinente.

Existen muchas herramientas de mantenimiento de blogs que permiten, muchas de ellas gratuitamente y sin necesitar grandes conocimientos técnicos, administrar todo el weblog, coordinar, borrar o reescribir los artículos, moderar los comentarios de los lectores...

Apuntándose a la blogmania, Microsoft acaba de presentar su nueva herramienta para la creación y gestión de bitácoras. Como es norma en los servicios ofrecidos por el portal de Microsoft, para poder utilizar MSN Spaces es necesaria una cuenta .NET Passport.

Tiene un sistema de comentarios, blogroll y herramientas para construir listas de libros o canciones. El blog puede ser privado (accesible para una lista de contactos), público o semiprivado, para la gente que tengamos añadida en MSN Messenger. También trae de serie la posibilidad de añadir fotos, para lo que ofrecen 10 MB de espacio.

Hay más de 20 templates para nuestro blog en MSN Spaces, pero todos con la misma estructura, cambiando los colores y algún que otro adorno, con especial afición por las margaritas. Está dirigido a gente novel, potenciando la facilidad de uso, y que van a apostar por una fuerte integración con otros servicios de MSN (Messenger, fotos, perfil del Passport). Ataca así al sector que podemos encontrar representado por Blogger, Blogia, DiarioGratis o Blogs.ya, quedando un sector representado por TypePad para usuarios más exigentes.

EXPLORER+FIREFOX



Sabido es que Internet Explorer es el navegador más utilizado por los usuarios de la web, por lo que muchos sitios de Internet incumplen las normas del W3C y están diseñados para trabajar con el navegador de Microsoft. Ésta es la única barrera que Firefox no puede saltar ya que no depende de él. Así que AOL Netscape ha decidido mover pieza en la guerra de los navegadores y cubrir ese hueco que quedaba abierto entre los grandes.

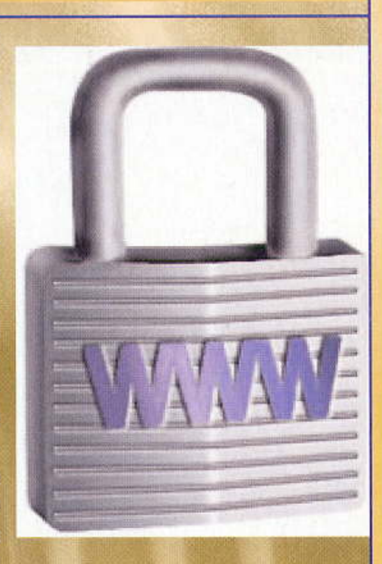
En los últimos meses se pasó de rumores que afirmaban que AOL estaba preparando un nuevo navegador basado en Explorer, a otros en los que se señalaba que habría un nuevo Netscape basado en FireFox. Finalmente ambos han venido a confirmarse hasta cierto punto, a pesar de su contradicción. Hay un prototipo del nuevo Netscape y está basado en FireFox 0.93, pero incluye la posibilidad de cambiar su funcionamiento para pasar a ejecutarse con el motor de Internet Explorer.

Es probable que AOL reciba un aluvión de críticas de los partidarios de FireFox. La grandes bazas de este navegador son ofrecer compatibilidad con los estándares y más seguridad que Internet Explorer. Con el nuevo Netscape se permite que los usuarios renuncien a ellas, pasando al modo Internet Explorer, mediante la carga de un control ActiveX en el navegador al modo del Avant Browser.

Veremos como acaba la segunda guerra de los navegadores: esperemos que gane el mejor.

RETRASO EN EL DNI ELECTRÓNICO

El ejecutivo español tiene la intención de invertir 100 millones de euros en el nuevo DNI electrónico.La puesta en marxa del proyecto piloto estaria prevista para comienzos de 2006 para tenerlo listo entre finales del 2007 y principios de 2008.
El ministro del Interior, José Antonio Alonso, declaró ayer miércoles ante el pleno del Senado en respuesta a una pregunta del senador socialista José Miguel Camacho sobre las novedades que presentará el DNI electrónico que tiene previsto implantar el Gobierno.
Alonso explicó que los costes estimados de la puesta en marcha de este nuevo documento para un período de cuatro años son de unos 100 millones de euros, de los que para 2005 ya están presupuestados 17.530.000 euros.
El ministro del Interior indicó que el DNI electrónico constituirá "una pieza esencial en la Administración electrónica puesto que va mucho más allá de un simple documento de identidad". El objetivo de este proyecto, señaló, es conseguir un documento de alta seguridad que además de garantizar la identificación de su titular "va a incorporar como ventaja decisiva la firma electrónica, lo que va a dinamizar el comercio electrónico y las infinitas posibilidades de la sociedad de la información".
Explicó que el DNI electrónico constará de un soporte físico, la tarjeta, que será de policarbonato, un material que el ministro consideró de alta fiabilidad desde el punto de vista de la seguridad.



El soporte electrónico del documento incluirá diferentes datos de identificación del titular, como son la huella digital y la imagen facial, e incorporará la firma electrónica.
Probablemente no dejaremos de ver nuevas formas de hacer menos anónima la red de redes; esperemos no ver nuevas formas de limitar la libertad de expresión, pero del DNI a esto hay un paso.

MICROSOFT CANVIA PIRATAS POR ORIGINALES

De acuerdo, el titular puede sonar algo sensacionalista, pero así es la vida misma. En una nueva estrategia contra la piratería, el gigante del software ha anunciado que concederá de manera gratuita licencias de Windows a aquellos usuarios que hayan adquirido ordenadores con software ilegal preinstalado. Bautizado con el nombre de "Counterfeit Project", el proyecto invita a los usuarios británicos a comprobar si sus programas son originales o no.
Microsoft se compromete a analizar la autenticidad de Windows XP "Home" o "Professional", y en caso de detectar que se trata de una copia fraudulenta sustituirlo por otro legal. La oferta promete al usuario no adoptar iniciativas legales contra el, y está limitada a cinco copias por persona.
Para conseguir la licencia los usuarios deberán enviar a Microsoft el recibo de compra del ordenador, junto a la carta de un testigo en el que se especifique dónde fue adquirido el ordenador.
Una estrategia con la que Microsoft pretende atajar el problema de la piratería de raíz, en el sector de los equipos originales. Es probable que esta medida reduzca los índices de piratería en la venta de equipos nuevos, al ir contra quien proporciona el software ilegal en lugar de atacar al sufrido comprador. Confiemos en que Microsoft no conozcan la máxima de los romanos, "Roma no paga a los traidores".





NFORCE5 Y RUMORES

Ya estan corriendo rumores sobre el próximo lanzamiento del nuevo chipset nForce5. De momento tan solo rumores sin confirmar, del chipset que nVidia está a punto de anunciar para plataforma Intel Socket775.
Soporte de FSB 800/1066Mhz, DDR2 667/533, 2 IDE, 10 USB 2.0, 1Gbit LAN, 4 S-ATA II Raid 5 y sonido 7.1 son la carta de presentación de dicho chipset.
Sólo nos queda esperar la confirmación o desmentido de dichas características en un futuro, esperemos que no muy lejano.

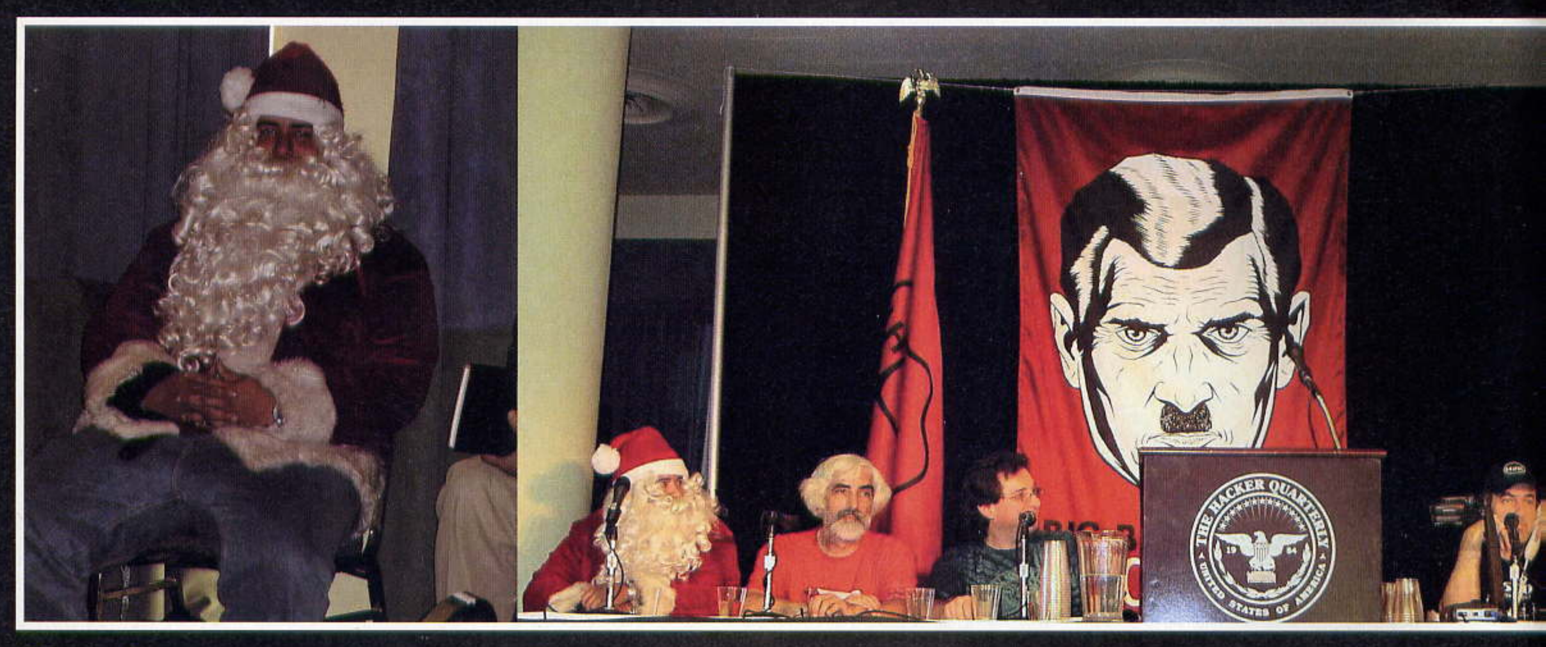
¡FELICIDADES, WALKMAN!

Efectivamente el pasado 6 de diciembre el Walkman cumplia 25 años. Quién no recuerda los primeros modelos que hicieron sonar esas cintas magnéticas que no solo contenian la música de la época, sino que también nuestras ilusiones. Sin duda se trató de uno de los grandes avances de la electrónica doméstica, que cambió el modo como estábamos habituados a escuchar música. En fin que nuestro compañero musical cumple un cuarto de siglo. Y comparado con los últimos modelos de mp3, MD, discman.... no se le ve muy en forma, los años pasan y se nota.

MOCOSOFT VENCE A MICROSOFT

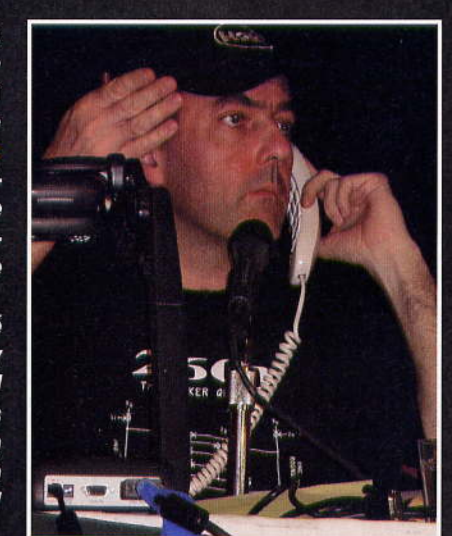
La OMPI recibió una denuncia de Microsoft solicitando la transferencia de dominios a favor del gigante de Redmond La Organización Mundial de la Propiedad Intelectual (OMPI) ha denegado a Microsoft la posesión de los dominios mocosoft.com y mocosoftx.com. Estos dos dominios en litigio continuarán en manos de su actual propietario, una sociedad radicada en Málaga. La OMPI considera que "los dominios tienen algún parecido", pero no hay confusión entre las dos marcas.

Ingeniería SOCIAL: lección



Esta conferencia, del pasado Hope en NY, muestra al trabajo las mentes más famosas de la Social Engineering:

La sesión en vez de ser teórica será práctica y toda la audiencia (la sala está atestada, con más de 600 personas) lo espera. **Emmanuel Goldstein:** *"cuando se hace Social Engineering es importante seguir una regla de comportamiento básica: no perjudicar nunca al objetivo de la conversación, porque es una persona que confía en nosotros. Podéis mentir y de hecho me presentaré como Scott Brown, y tendré una excusa y un objetivo en mente. Para obtener el resultado final procederemos por pasos obteniendo un poco de información cada vez. Nuestra víctima es Taco Bell (una cadena de fast food orientada al TexMex)."*



Primera llamada

EG: *"Soy Scott Brown de la sede central, resulta que habéis tenido un problema en el registro de caja... ¿Puede darme el NIF de la tienda para verificar?* [el NIF de la tienda es el de alta, normalmente escrito en los recibos]" ... Un palo al agua: el empleado no sabe el número...

Segunda llamada

EG: "... [presentación habitual]. *¿puedo hablar con el supervisor? ... Ah, hola Paul, soy Scott, Scott Brown de la sede central, nos han indicado problemas y tenemos que verificar las cajas registradoras...* [charla sobre los frecuentes problemas a verificar, que ya no se hacen las cosas como antes, que en Pasadena hace mal tiempo y por fin...] *¿Qué registradoras usáis, las viejas CR o las nuevas?*

Paul: *"Aquí hemos tenido siempre las CNR"*

EG: *"¿CNR, 2100 o las otras, puedes verificarlo Paul, por favor?"*

Paul: *"Llevan escrito 1100"*

EG: *"OK Paul, buen trabajo, gracias."*

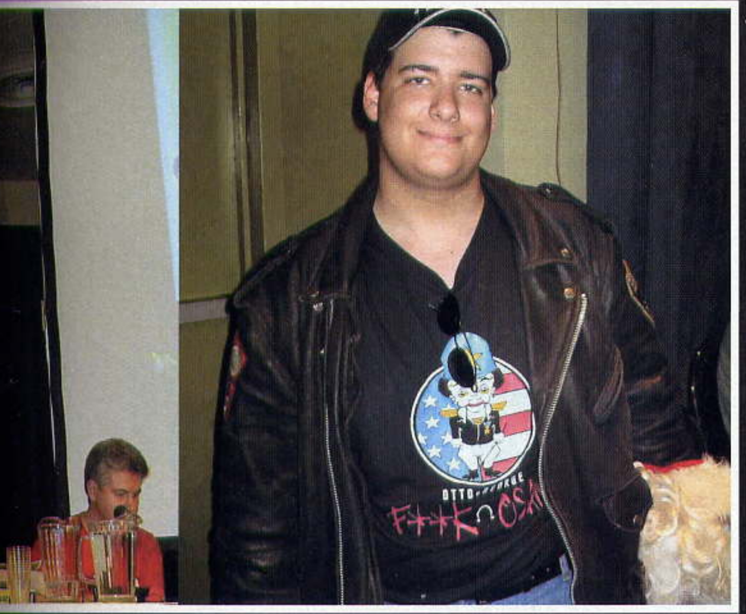
Tercera llamada

EG: "... [presentación habitual]. *¿puedo hablar con el Supervisor? ... Ah, hola Mike, soy Scott, Scott Brown de la sede central y me han pedido que actualice las cajas registradoras, ya sabes, las viejas CRN 1100. Se estropean mucho y conviene actualizarlas, sino tarde o temprano alguien tendrá problemas* [observad la sutil amenaza que suena como: ya te lo he dicho; si lo rechazas y sucede algo será cosa tuya...]"

Mike: *"¿Qué hay que hacer?"*

EG: *"Tranquilo, son 2 minutos, pongamos 5 por precaución: de las 9:00 a las 9:05 no uséis las cajas registradoras, ya están conectadas al teléfono y podemos hacerlo todo desde aquí, basta con que no hagáis resguardos*

en DIRECTO



¡Emmanuel Goldstein, Kevin Mitnik y Cheshire Catalyst!

durante esos cinco minutos; podéis entrar pedidos pero no hagáis resguardos..."
Mike: *"Está bien Scott, de 9:00 a 9:05. Gracias Scott."*
EG: *"Como véis, ha sido fácil y no hemos causado daños, sólo una pequeña molestia de 5 minutos a las nueve...* [...]

Otro llamada a BlockBuster, ahora pasándose por Scott B. Se obtiene el número de teléfono y la dirección de otro usuario que se llama Scott como él pero con otro apellido que empieza por B.
EG: *"Scott es un nombre muy común pero sólo con la inicial tengo muchas posibilidades de hallar una persona buscada porque muchos nombres los ha listado el supervisor por sí solo. Ahora probamos algo más difícil: buscamos el número de teléfono del call center de Bombay de Mastercard."*

Llamada al número 800 de Mastercard ...

Va mal: sin el número de tarjeta no avanzamos.
Kevin Mitnik: *"¡En American Express no se requiere el número!"*
EG: *"Llamamos a Amex...* [la voz grabada pide el número de la tarjeta] *pulsamos 0* [la voz grabada pide nuevamente el número de la tarjeta] *pulsamos 0* [la voz grabada pide nuevamente el número de la tarjeta] *pulsamos 0* [la voz dice que nos pasa con un operador, la platea aplaude].
Buenos días, soy Scott Brown de la MCI de New York [noto carrier telefónico americano] y nos han llamado por problemas en la conexión internacional: parece que cuando llaman el número 800 no llegan a Bombay en India sino a otra parte "
Operadora Amex #1 *"Esto es Manila, Filipinas"*
EG: *"¡Lo sabía, la base de datos está patas arriba! Para resolver el problema, ¿me da el número de teléfono de su centro, me dice que es Manila, verdad? "*
[la operadora no tiene el número, nos da la dirección pero no tiene el número exacto, y nos pasa al supervisor.]
Supervisor Amex #1 *"[...] no tengo el número, le paso con la sección técnica"*
Supervisor Amex #2 *"[...] Scott, qué ticket number habéis asignado al problema?* [la audiencia guarda silencio, éste es un momento difícil ...]
EG: *"Sabes Chris, estamos intentando resolver el problema antes de que empeore, aún no es grave y no le hemos dado un número todavía"*
Supervisor Amex #2: *"OK, Scott entiendo, te paso a la sección extranjera"*
EG: [directo al público]: *"veréis, el ticket number tiene un formato definido por cada compañía, yo no sabía cuántas letras y números dar y por ello ha sido mejor decir esto que decir un número al azar.*
Utilizad una voz aburrida y un tono de confidencialidad como diciendo: ¡sabes si asignamos el ticket luego es mejor para nosotros y para vosotros así que si lo hacemos así es mejor para todos! "
Supervisor Amex #3,4,5,6 [paso por paso]
EG: [directo al público]: *"A veces es necesario dar muchos pasos"*
Supervisor Amex #7: *"Hola Scott soy Beri [la voz tiene un claro acento indio, el público está en ascuas] ¿en qué puedo ayudarte?"*
EG: [repite la historia de la base de datos y de las llamadas que llegan a Manila en vez de a Bombay] *"¿Puedes darme el número directo del call center?"*
Supervisor Amex #7: *"Desde luego Scott toma nota: XXX YYY XXXXXX"*
EG: *"XXX es el prefijo para la India y YYY el de Bombay?"*
Supervisor Amex #7: *"Exacto"*
EG: *"¡Gracias Beri!"*

[¡Fin de la llamada y gritos de alegria en la sala de conferencias!]

También los expertos en Social Engineering tienen algo que aprender. ¡Este muchacho vestido de papá noel está tranquilamente sentado en el palco y tomó la palabra sin que nadie se lo pidiera ni objetara nada!

MAESTROS EN CLASE

Pero los maestros de Social Engineering han aprendido una lección a su vez: ¿veis a ese curioso personaje que va vestido de papá noel? ¡Ahora lo veis en el palco sentado cerca de Cheshire Catalyst y hablando también por el micrófono! ¿Quién era? Nadie en especial, solamente un muchacho que imaginó, precisamente, que así nadie le haría preguntas, ¡se trata de un verdadero campeón de Social Engineering! ¡También los maestros a veces aprenden una lección ;-)

Órdago al casino

¿Qué hacer cuando una banda de piratas de quién sabe dónde toma como rehén tu sitio? A alguien le ha sucedido y no siempre se han librado de manera indolora...



↑ ¡Tras los ataques a los casinos online no son sólo los jugadores quienes se quedan en bragas!

En julio les capturaron. Una banda rusa ponía fuera de combate los servidores de las agencias inglesas de apuestas, mediante ataques DDoS, y luego pedía dinero para dejar de hacerlo.

La National Hi-Tech Crime Unit británica colaboró con las autoridades rusas para localizar a los tres culpables. De entre 21 y 24 años, pedían sumas de entre diez y veinte mil dólares, con máximos de 55 mil. Pero se necesitó tiempo y, desde la denuncia en octubre de 2003, los piratas consiguieron causar daños de cientos de miles de euros o más. Por fin se descubrió que también habían intentado hacer chantaje a los postores de EE.UU. justo antes de la Super Bowl, la final del fútbol americano.

No todo el monte es orégano

Pero a otros no les ha ido tan bien. Hablamos de Multibet (http://www.multibet.com), sociedad de apuestas que lidera el australiano Terry Lills, que opera en un decena de países.

Los chantajistas aparecieron y pidieron a Lills más de 15 mil euros a cambio de protección. Él les mandó al infierno y ellos, cinco minutos después, le bloquearon el sitio con un ataque DDoS: un mazazo que bloqueó el negocio durante casi tres semanas provocando pérdidas incalculables.

QUÉ ES UN DDOS

DDosS significa Distributed Denial of Service. Ataque en el que una multitud de sistemas comprometidos (por ello se llama distribuido) bombardea a su pesar un blanco, que se hunde bajo un número de paquetes excesivo para su capacidad y ya no puede llevar a cabo sus funciones.



Finalmente Lills capituló y pagó. Ahora trabaja, pero cada mes envía un giro a una cuenta lituana mediante un pago de Western Union.

Mientras tanto la policía australiana rastrea las huellas de los maleantes, en colaboración con varias fuerzas del orden europeas. Cuando le encuentren es probable que sea un buen golpe, porque para bloquear tres semanas un sitio es preciso tener un buen ejército de zombis.

PCs ignorantes y dormidos

Los zombis son, en la jerga, los ordenadores usados para el ataque. Son miles, propiedad generalmente de ciudadanos ignorantes o bien empresas con pésimos administradores de red. El chantajista toma posesión con un gusano y, en su momento, desencadena el ataque. Según estimaciones, el 1% de equipos en Internet puede estar comprometido. Tal vez nuestro equipo se usa en este preciso instante para desencadenar un ataque, junto con otros mil o diez mil. Diez mil zombis son un patrimonio, que le cuesta a su dueño también algunos miles de euros.

La nueva frontera del chantaje informático son ahora los casinos online. Dan mucho dinero, dependen completamente del web, los propietarios los abren en paraísos fiscales donde no pagan impuestos pero donde es difícil obtener colaboración de la policía.

La eterna partida de policías y ladrones actualmente va a favor de estos últimos. Esperamos que la tendencia se invierta, antes de encontrarnos bandas de extorsionadores de tres al cuarto que amenacen sitios de la gente normal y corriente.

No Son Sólo Muertos

Por zombi se entiende un ordenador infectado con un gusano o un troyano, dominado remotamente para lanzar ataques DDoS sin que lo sepa el propietario.

NHTCU y policías diversas

En la National Hi-Tech Crime Unit (http://www.nhtcu.org/) nació en 2001, cuando el gobierno británico tomó nota de un informe que denunciaba los altos riesgos debidos a la actividad de criminales informáticos. En nuestro país contamos con dos alternativas: la BIT (Brigada de Investigación Tecnológica) dependiente del Cuerpo Nacional de Policía en el sitio http://www.mir.es/policia/bit/, y la Guardia Civil de delitos telemáticos, en el sitio web http://www.guardiacivil.org/seguridad/index.jsp.

WiFi Shootout!

55,1 millas. Ésta es la distancia que representa el nuevo récord establecido el sábado 31 de julio a cerca de 50 millas de Las Vegas en ocasión del segundo WiFi Shootout

STORY BOARD



A más de 80 kilómetros de distancia de Las Vegas y con 112 grados Fahrenheit (44,5 grados centígrados) he aquí la cuenca elegida para la segunda prueba del WiFi Shootout. Según los organizadores la línea del horizonte, usando la colina tenía que ser ampliamente suficiente: 55 millas. ¡Error!



Este equipo de Seattle ha instalado en la colina dos antenas comerciales, una omnidireccional y otra direccional, ambas amplificadas con aparatos comerciales Cisco. Al fondo a unas 25 millas se encuentran sus compañeros con la unidad móvil.



El calor y el viento fueron los enemigos de la competición. El cómodo parasol yace desmontado por tierra dado que el viento no permitió su instalación en la colina. La cobertura del móvil en medio del desierto es increible: estos viejos teléfonos analógicos funcionan, mi GSM se murió a las treinta millas.



"Se necesitaron catorce viajes desde allá abajo para traer todos los aparejos sobre la colina; ayer estábamos tan cansados que nos dormimos antes de que llegaran las pizzas y nos hemos despertado esta mañana todavía vestidos". Sin lugar a dudas, si un hacker no es despertado por la pizza es que está realmente muerto



La antena fija mira a 55,1 millas sobre una lengua de tierra hacia el fondo de un socavón, sobre las montañas por la otra parte de la cuenca, donde se han aventurado los otros con el carrito. Team P.A.D (Parabolic antena Designer) es el nombre que el grupo ha escogido para la competición.



Estas dos muchachas vienen de Washington DC. Han ganado el premio para la antena más innovadora, realizado con un tipo de plástico de aluminio que se suele usar para mantener el calor fuera de la habitación de las máquinas. Desgraciadamente no han hecho las cuentas con el calor infernal del desierto y la estructura de la antena ha cedido, obligando a mantener la antena abierta con las manos. Poco más de un kilómetro la distancia cubierta sin amplificación.

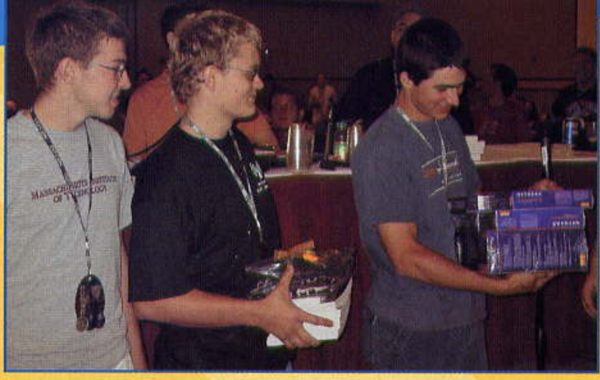
Tres muchachos (de hecho cuatro, incluido uno que no ha podido ir a Nevada) de Ohio de menos de 19 años se han hecho con el premio Uber Hacker que le da acceso de por vida a los próximos DefCon, construyendo un par de antenas parabólicas de unos tres metros de diámetro.
El récord de sistemas amplificados se estableció en 2003 por Alvarion y la Swedish Space Corporation que establecieron contacto con un globo aerostático a más de 310 kilómetros de distancia. los problemas de la curvatura terrestre y la misma atmósfera hacen que el enlace con el globo sea más simple que entre dos estaciones de tierra. Se estima que la máxima distancia posible tiene que ser de unos 400 kilómetros.
Pero los chicos de Ohio, alcanzada la máxima distancia que el terreno permitía, detectaron una insólita calidad del enlace y entonces tuvieron la loca y estrafalaria idea de eliminar el amplificador, sólo para reirse un rato, y en cambio: ¡milagro! Nuevo récord del mundo para una conexión no amplificada: 88,67 Km.

Salieron a la caza de conexiones no protegidas. Y han llegado hasta aquí

Es interesante indicar qué ha llevado a los muchachos a DefCon y a participar en el segundo WiFi Shootout. Su proyecto original era ir darse una vuelta por Cincinnati en busca de conexiones WiFi no protegidas. Una vez identificada la conexión, contactaban con el usuario y se ofrecían para protegerla. Los resultados de esta actividad han sido interesantes, especialmente cuando las personas, mosqueadas por la petición, llamaban la policía o les echaban con malos modos.
Buscaban un uso para las parábolas y helos aquí conduciendo dos mil millas con una antena de tres metros (dos metros y 89 centímetros exactos) sobre un remolque.
http://www.wifi-shootout.com/



↑ Estos son los ganadores del año pasado, ASLRulz. Su récord de 35,2 millas ha sido pulverizado y además tampoco ellos hicieron las cuentas con el horno del desierto: la pistola de cola aquí no funciona y no consiguen pegar la red a los soportes. Al final usarán montones de esparadrapo y no llegarán muy lejos.



↑ Team P.A.D. (Parabolic Antenna Designer). De izquierda a derecha Justin Rigling, Andy Meng y Ben Corrado retiran el montón de premios reservados a los ganadores de las categorías para antenas autoconstruidas amplificadas y no.

↓ El remolque con el disco. ¡Imaginad recorrer más de 2000 millas con eso! Pero ahora imaginad que os lo encontráis aparcado delante de casa con un muchacho que balbucea algo sobre problemas en vuestra conexión WiFi; ¿no llamaríais vosotros también rápidamente a la policía?



↓ Para el regreso el equipo desmonta todos los trastos. Les esperan casi dos días de viaje antes de llegar a casa. ¡Mirad las estructuras de hierro necesarias para soportar la antena e imaginad lo cansado que es subirlas a la colina con 40 grados bajo el sol!



← Las frecuencias del WiFi están MUY cerca de la frecuencia de resonancia del agua. Especialmente los ojos pueden llegar a sentir las consecuencias de maniobras equivocadas o arriesgadas con antenas amplificadas a alta ganancia.



¡PENTIUM A 6 GHZ!

Nuestro PC ha sido diseñado con límites. Que queremos superar. Uno de los principales problemas es el calor generado por los componentes, y el procesador el primero. Si hacemos que funcione a los valores declarados por el fabricante, lo usaremos como todos: estamos en la media. Pero nosotros queremos más, no nos conformamos. Los componentes, sabido es, no se hacen funcionar al límite de su capacidad. Y nosotros queremos ir más allá del límite.

Todos conocemos el ruido de nuestro PC cuando está en marcha: son los ventiladores. Todos los componentes electrónicos se calientan. Cada componente dentro un procesador se calienta. Y en un procesador moderno, hablar de algo como un millardo de transistores en unos 2 cm cuadros da escalofríos. Por ello si no enfriamos nuestro procesador, se quema.

Con mayor razón si pisamos el acelerador y llevamos nuestro procesador a trabajar más allá de los límites declarados. Así, los intentos de sobrepasar cada límite aparecen como hongos. ¿Con qué resultados? Bueno, ver para creer. Hay quien ha superado todo límite: un Pentium 4 forzado a funcionar más allá de los 6 GHz es el récord actual absoluto.

El problema principal es enfriar la CPU con un sistema que pueda tragarse lo más rápido posible el calor pro-



↑ *El récord absoluto: ¡6 GHz gracias al nitrógeno líquido! (by Macci, del equipo Akiba, www.akiba-pc.com)*



SI QUEREMOS PROBARLO

Bueno, si nuestro fin es evitar un poco del ruido de los ventiladores que enfrían los modernos procesadores, no es aconsejable adoptar medidas tan extremas como el hielo seco o el nitrógeno líquido.

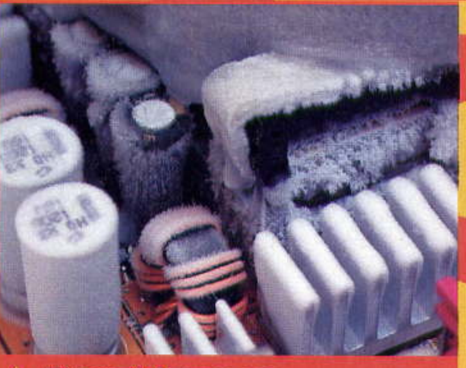
Podemos quedar satisfechos utilizando sistemas de enfriamiento más clásicos, que funcionan sobre el principio de los radiadores de agua de los automóviles. Se hace circular agua, o un líquido refrigerante, dentro de un serpentín y sobre el procesador. El líquido absorbe el calor generado y lo pasa al serpentín, que en general también se refrigera con un ventilador, pero a un número de revoluciones tan bajo que el ruido es imperceptible. En estos casos conviene usar un sistema de refrigeración que prevea la absorción del calor sobre el procesador, o sobre los demás componentes principales de la placa base. Una búsqueda

El overclocking extremo ha llegado a poner el Pentium en nitrógeno líquido. He aquí alguna imagen y alguna solución más abordable.



CPU refrigerada con nitrógeno líquido, pero los otros chips requieren una refrigeración al menos de agua.

en Google nos dará una panorámica decididamente amplia. Atención de todos modos al ruido.
Si el factor de ruido es el que nos empuja a enfriar nuestro PC con sistemas alternativos, podemos tomar en consideración este kit: www.zalman.co.kr que no incluye ningún ventilador y es hasta bonito, aunque, evidentemente, estorba un poco.



↑ El problema es el enfriamiento de todo lo que está cerca: un experimento que durará poco... (foto Tom'sHardware, www.tomshw.it)

ducido. Esto significa crear una diferencia de temperatura entre el interior y el exterior del procesador lo más alta posible. O sea, hallar un sistema de enfriamiento a la temperatura más bajo posible.
Se han hecho los primeros intentos con anhídrido carbónico sólido, el llamado hielo seco. El hielo seco pasa directamente del estado sólido al gaseoso alcanzando temperaturas de -78 grados. Usar materiales a estas temperaturas no es fácil. Los problemas que pueden surgir sólo con el hielo seco son:
a) la dificultad de manejarlo. Indispensables los guantes que resistan a temperaturas tan bajas, porque tocarlo con las manos provoca quemaduras profundas y la piel se pega, literalmente, a superficies tan frías;
b) es necesario seguir añadiendo hielo seco al sistema, porque se sublima de prisa. Un Pentium en condiciones normales, a 2,2 Ghz, disipa ya más o menos como una bombilla de 60 W, por lo que el hielo seco se consume de prisa. Además enfria también el ambiente circundante, lo que contribuye al consumo;
c) en un ambiente algo húmedo el hielo seco genera escarcha y el agua presente en el aire recubre los componentes presentes en la placa base. Esto puede disminuir la resistencia entre puntos diversos, incluso cortocircuitos. Por ello hay que aislar cuidadosamente la zona. Además aumenta la corrosión de las partes metálicas (como los pines de los circuitos), y el estrés mecánico al que se ven sometidos los componentes.
Se ilustra un método en el link www.hwtweakers.net/postt1369.html

Mediante el enfriamiento por hielo seco hay quien ha conseguido obtener un overclocking del procesador de casi 1 Ghz, llegando así a alrededor de 4 Ghz.

Cada vez más

[illegible]seguimos bajar más la temperatura, podemos batir nuevas barreras. Pero las cosas se complican mucho y el tema se acerca más al laboratorio de una universidad que al overclocking casero. Por lo menos por las sustancias en juego. Lo más simple para bajar drásticamente la temperatura es usar nitrógeno líquido. Vendido en contenedores aislados, recipientes de Darwin o termos, es la última barrera del overclocking ¡porque alcanza nada menos que unos 196 grados centígrados bajo cero! Grandes ejemplos de experimentaciones en este sentido se encuentran en www.akiba-pc.com/article.php?34.0, donde se ha batido el récord absoluto de overclocking, ¡llevando de 3,2 a más de 6 Ghz la frecuencia de funcionamiento de un Pentium 4!
Y si queremos divertirnos viendo un



↑ Un pulpo de refrigeración... (foto Elma)

experimento completo, y filmado, de estas pruebas, tenemos que descargar el grandioso filme en la dirección www.de.tomshardware.com/guides/cpu/20031230/images/thg_video_11_5ghz.zip que es el experimento exitoso de superar los 5 Ghz hecho por los fans de Tom's hardware de donde proceden las fotos que os mostramos.
Para mirar el filme es indispensable haber instalado un codec DivX, que descargaremos gratuitamente en la dirección www.divx.com/divx/download.
Señalemos que también el equipo italiano ha intentado batir el récord: todos los detalles están en la dirección www.tomshw.it/howto.php?Guide=20040610.

Domar el CENSORWARE




¿Libres o seguros? Tal vez los términos del problema no son exactamente estos. De todos modos los programas que limitan la navegación son inútiles. He aquí por qué...

EL TRUCO MÁS SECRETO

Incluso NetNanny parece tener una backdoor, dejada por los programadores. Prueba a usar el password "~frontdoor" (sin comillas). A veces funciona.



Al oír hablar de Net-Nanny nos da la risa. Aparte de tener un nombre tan infantil, éste y sus parientes aparecieron para evitar caer en lugares considerados inoportunos u ofensivos. ¿Pero es exactamente así? En realidad no existe un método técnicamente seguro para evitar caer entre los tentáculos de las miserias humanas: al contrario, además de los daños de la censura imperfecta los programillas en cuestión llevan consigo también el daño de limitar al por mayor la libertad de navegar. Bloqueando, por ejemplo, también lugares donde se habla de cáncer de mama de modo simple y explícitamente claro, o bien donde se explica la transmisión mediante relaciones sexuales del SIDA, y así sucesivamente. Si lo pensamos bien, no poder usar algunos términos -porque en esto se basan la mayor parte de los programas en cuestión- es de por sí un enorme límite a la disponibilidad de información, en un mundo en el que todo sucede y todo puede suceder, en cualquier parte. Y todo se regula ya frecuentemente y de modo provechoso en la red, en alguna parte. OK, entonces veamos cómo liberarnos de esta inútil censura.

Como liberarnos de NetNanny

La versión 4.0 la eliminamos de Inicio > Ejecutar. Escribimos msconfig para iniciar la utilidad de configuración del sistema. Vamos a Inicio y quitamos la marca de "nntray.exe" y "NNSvsc", luego reiniciamos. Hecho. O bien lo deshabilitamos al momento directamente del administrador de tareas (Ctrl-Alt-Supr). Vemos la tarea de OCRAWARE o Wnldr32 (depende de la versión) y un clic sobre Terminar proceso será suficiente. Para eliminarlo del todo, buscamos el archivo C:\windows\system.ini.
Hacemos una copia de seguridad con otro nombre, que guardaremos. Nunca se sabe. Lo abrimos con el Bloc de notas y buscamos el encabezamiento [boot]. Debajo tiene que haber algo como Drivers= seguido de una lista, entre ellos wndrv16.dll. Lo borramos (¡sólo éste!). Guardamos el archivo y listos.
Si también queremos limpiar los archivo de log, buscamos y borramos Wnn3.log en el directorio de Net Nanny. El archivo está cifrado, por lo que debe eliminarse en bloque, no se puede modificar.

Con SurfWatch se hace así

Para los que no tienen miedo de tocar los registros del sistema, he aquí cómo se hace. Abrimos la carpeta de Inicio y eliminamos el enlace a SurfWatch y el de SurfWatch Updater. Abrimos el archivo win.ini y cambiamos la línea

```
load= C:\CO_RO_NT\surfctl.exe
```

dejando solamente

```
load=
```

Vamos a Inicio > Ejecutar > regedit y borramos la clave GraphicsFilter, que es una subclave de

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\
```

El valor de esta clave será

```
C:\CO_RO_NT\surfctl.exe.
```

La eliminamos.



Reiniciamos el equipo en modo DOS (F8 al arrancar).
Nos vamos a la carpeta c:\windows\system\directory y escribimos:

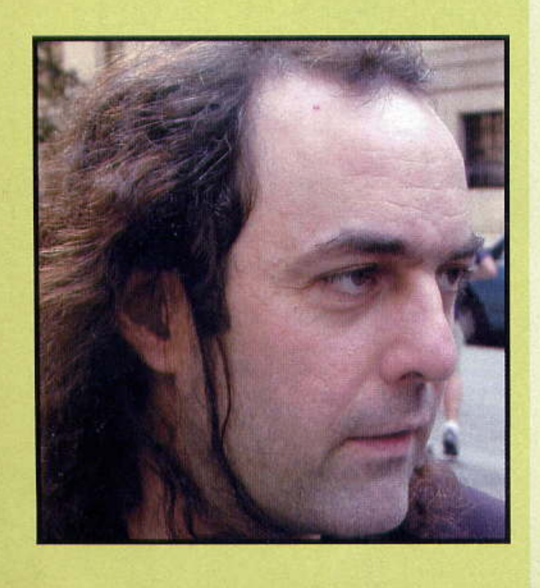
```
attrib -h -r -s system.drv
attrib -h -r -s net.drv
move system.drv system.bak
move net.drv system.drv
```

Escribimos win para reiniciar Windows. Si aparece algo como: Windows está ejecutando uno o más programas de MSDOS... escribimos simplemente exit.
SurfWatch estará ahora deshabilitado. Si rehacemos los pasos al revés lo podremos recuperar. de nuevo. Aunque ¿quién lo necesita? En fin, hay ocasiones para todo...



MR. 2600: EMMANUEL

Su especialización: Hacker information. Pero si oímos un tono a 2600 hercios, sin duda alguna ¡es él!

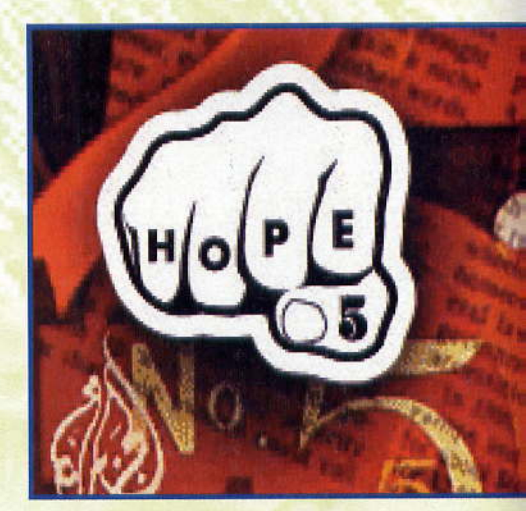


New York City, 31 de agosto de 2004, cerca de Union Square están marchando ruidosos manifestantes contra la convención republicana. Ante unas elecciones, ya se sabe, puede suceder de todo y una implacable cámara fija en la esquina con la calle 16 registra la llegada de la policía. 150 manifestantes marchan encerrados en pequeños furgones. La manifestación se disuelve entre los gritos de los participantes que huyen. Pocos diarios en el mundo han dado la noticia. Lo normal, cosas que pasan. Pero en la redacción de "2600 - the hacker quaterly", reina la agitación. Entre los apretujados personajes detenidos por la policía, está su histórico fundador: Eric Corley, más conocido como Emmanuel Goldstein. Las últimas noticias lo dan como libre de nuevo tras 32 horas de celda y comprobaciones. No debe haber sido fácil, dados los antecedentes.

A principios de los noventa, en efecto, la revista y su fundador acabaron ante un tribunal de acusado por el MPAA, la potente asociación para los derechos cinematográficos americanos, de "distribución de software ilegal". La acusación a Goldstein era permitir la distribución de DeCSS, la famosa utilidad para decodificar DVD. Convicto en una resolución positiva de la causa, será obligado en cambio a ir derecho a la corte del distrito de Nueva York, poco después del 15 de agosto de 2000. Goldstein tiene que quitar el software de su servidor y pagar las costas procesales.

Hacker teórico y literato

Criado en Long Island, Nueva York, se apasiona inmediatamente por la tecnología, pero queda fascinado por el web: intocable. Vive del hacking sin ensuciarse las manos, lo teoriza sin tocarlo. ¿Pero es exactamente así? Enamorado de la radiofrecuencia e inventor de conductores radiofónicos, cuando se inscribe en la State University of New York se convierte en el matarife de la radio de la universidad. Paralelamente a la cultura hacker, en aquellos años se difundía la cultura hippie con elementos destacados como Abie Hoffman. Precisamente tal figura será un punto de referencia importante para Goldstein.



HOPE, Hacker On

Siempre más teórico que práctico (al menos en apariencia), poco después Emmanuel será uno de los nombres más escuchados y respetados en el entorno hacker, por su espíritu de propuesta, las muchas campañas pro-hacker y la información continua en varias revistas en las que colaboraba.

Eric funda la revista de hacker por excelencia: "2600: The Hacker Quarterly". Especializada en phreaking e ingeniería social, el nombre de la revista proviene de la frecuencia del tono emitido por los teléfonos en las conexiones interurbanas en EE.UU.: 2.600 hercios.

GOLDSTEIN



Planet Earth...

Un grupo de 60 mil

La revista se impuso enseguida pillando una buena franja del mercado underground: unos sesenta mil lectores fieles esparcidos por todo el mundo. Así se convirtió automáticamente en la voz más autorizada entre los hackers y la más vigilada por parte de las autoridades y los tribunales americanos.

También porque, desde su creación, 2600 sigue de cerca las vicisitudes más importantes del hacking y lanza pesadas campañas contra la autoridad. En cuanto puede, Goldstein lanza acusaciones contra las sentencias emitidas por los tribunales, que considera injustas y exageradas. ¿Un rebelde a toda costa? Tal vez, pero no siempre tiene toda la culpa. Como en el caso de Craig Neidorf, conocido como Knight Lightning. El muchacho consiguió entrar en los sistemas del Bell South, extrayendo de ellos un buen paquete de lo que se consideraban secretos industriales.

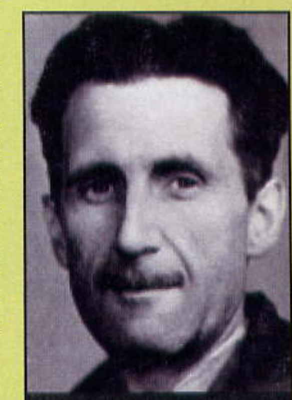
Dado que esta afición, ciertamente, no resultó particularmente grata a quien había invertido en aquellos secretos millones de dólares, fue detenido y procesado con dureza. ¿Cómo terminó todo? Fue absuelto, lo creamos o no, porque la revista 2600 demostró que el material que Knight Lightning había sustraído de los sistemas Bell South podía comprarse regular y legalmente por pocos dólares. Tal vez Knight no lo había planeado así, pero esa es otra historia.

Las últimas luchas

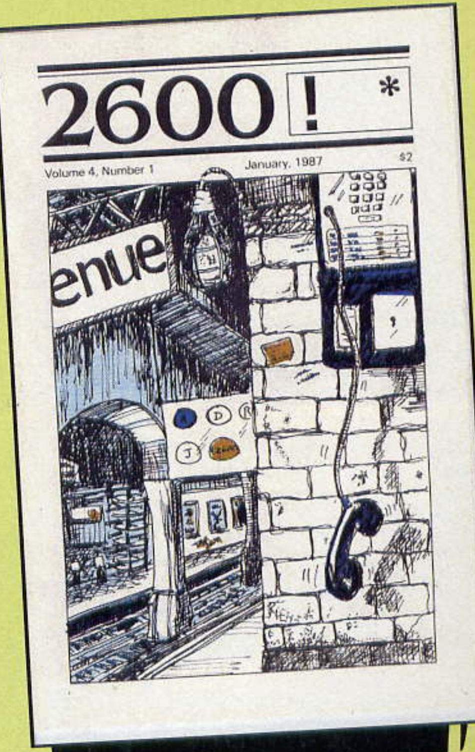
Agosto 1994: 2600 invita a todos quienes siguen la revista a participar en la primera conferencia planetaria de hackers, HOPE. Durante el Hacker On Planet Earth se habla de todos los aspectos del hacking, de las últimas vicisitudes en el ámbito judicial, se produce la presentación de nuevo software, se encienden discusiones técnicas, pero sobre todo se habla del Cóndor. Kevin Mitnick está en prisión y el HOPE lanzará el primer grito de "Liberad a Kevin". En 2000, el 21 de enero, Eric Corley se presenta delante de la cárcel donde pocos minutos después es soltado finalmente el Cóndor. Goldstein no se resiste al micrófono y, en directo en "Off the Hook", una transmisión que se ha hecho famosa y fue transmitida por la estación de radio WBAI, habla y hace hablar a su huésped de excepción, que en los años de cárcel ha podido ciertamente preparar un buen discurso. **Pero los años pasan para todos.** El espíritu batallador de algunos se debilita y, salvo alguna batalla sostenida aún en la trinchera, hoy estos son personajes de un mundo que ha cambiado. Nos lo ha demostrado un Mitnick en americana y corbata, consultor de seguridad, que en la quinta conferencia HOPE se exhibió con Goldstein en un extraordinario show dialéctico.

Orwell 1984

Goldstein es precisamente el nombre que George Orwell dio al protagonista de "1984", la figura rebelde, el que escribió "The Book", El Libro, que incluía todas las herejías, que se había hecho circular clandestinamente por todas partes. Hoy hay hasta quien compara la figura originaria de Goldstein con el diablo, o Bin-Laden. La discusión sigue abierta...



El autor de 1984, creador del Gran Hermano.

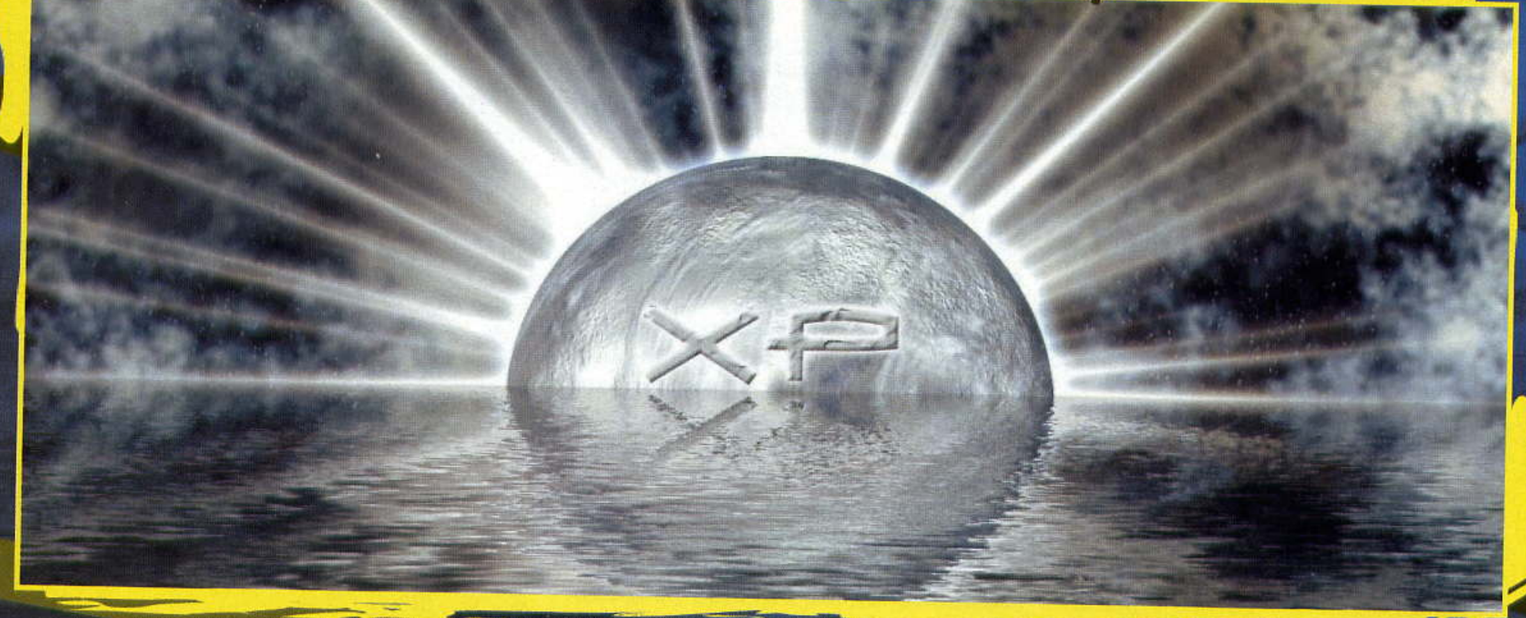


2600 ! *

Volume 4, Number 1 — January, 1987 — $2

Una de las primeras cubiertas de la mítica revista 2600

TRUCOS y SECRETOS de Windows



Windows nunca deja de sorprendernos y de dar posibilidades de ejercitar nuestro deseo de hacking

Secreto numero uno: inegativo!

Supongamos que acabamos de adquirir un nuevo PC y, dado que somos hábiles expertos y no queremos perder nada de los nuestro trabajo anterior, hemos transferido todas las carpetas del viejo PC al nuevo. Incluida una carpeta de nombre Escritorio, que hemos llenado por comodidad con todo lo que teníamos en el escritorio del equipo viejo.

La colocamos en el escritorio del nuevo PC, para tenerla así a la vista.

Resulta que:

- si con un clic intentamos abrir un nodo del directorio, o sea hacemos clic sobre el símbolo (+) que indica que debajo de la carpeta hay otros objetos, la subcarpeta no puede abrirse;
- la carpeta de escritorio (la verdadera, del nuevo equipo), puede replicarse muchas veces;
- en todas las demás carpetas, o en algunas de ellas, puede cambiar el nombre con caracteres espurios y casuales;
- nos aparecen una serie de mensajes más o menos de este tipo:

"F: \Documents and Settings\Administrador\Desktop\Desktop\Desktop se refiere a una ubicación no disponible. Podría estar en un disco duro de este equipo o en una red. Verificar

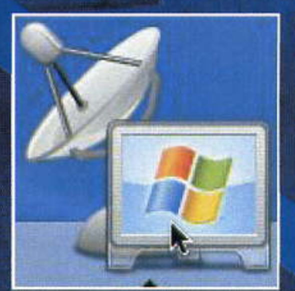




que el disco se ha insertado o que se tiene conexión a Internet o a la red, y probar de nuevo. Si sigue sin hallarse, puede haberse movido la información a una ubicación diferente".

Estos errores pueden aparecer juntos, separados o no aparecer. ¿Qué sucede? Simple: hay que evitar siempre crear una carpeta con el nombre de escritorio en el escritorio, so pena de provocar demencia precoz en el explorador de Windows. Palabra de tantos usuarios que se han encontrado en situaciones límite del absurdo y palabra de Microsoft, que avisa en la nota técnica disponible en la dirección: http://support. microsoft.com/default.aspx?scid=kb;en-us;323681&Product=winxp#appliesto

Truco numero dos: positivo



Cuando trabajamos con el escritorio remoto, podemos dar al equipo remoto la orden de apagarse.Basta con abrir el Bloc de notas, o algo parecido, y escribimos esta línea de instrucciones:

```
(newActiveXObject("Shell.Application")).ShutdownWindows();
```

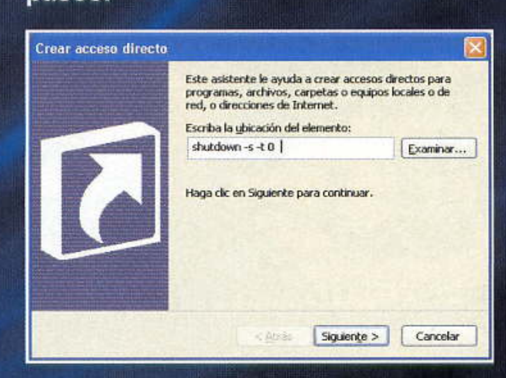
Después guardamos el archivo en el escritorio con el nombre RemoteShutdown.js. Un doble clic activa el apagado del PC.

Truco numero tres: ¡positivo!

¡Eliminemos todo lo que podamos! Ganaremos espacio en disco y velocidad de proceso. Una carpeta a vaciar sin piedad en Windows XP es C:\Windows\Prefetch. Un buen cepillado no hace ningún daño y los archivos necesarios se recrean automáticamente de nuevo, hasta la próxima limpieza.

Truco numero cuatro: positivo

¿Apagar velozmente el PC con Windows XP? Fácil, basta seguir estos pasos:



- clic secundario en el escritorio, Nuevo > Acceso directo
- en la ruta escribimos:

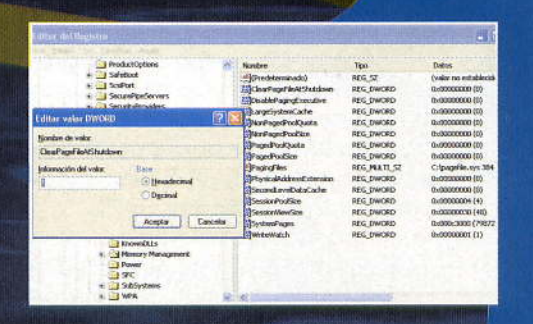
```
shutdown -s -t 0
```

(para evitar errores lo diremos más claro: shutdown[espacio]-s[espacio]-t[espacio]cifra cero).

- un clic en Siguiente y lo llamamos Apagar, o como queramos.
- dos clics sobre el icono creado en el escritorio y el PC se va a la cama.

Secreto numero cinco: positivo

En el archivo de intercambio de Windows se guardan, como en una caché, los datos reasignados de la RAM, cuando ésta no basta o se requiere más espacio. Windows está preconfigurado para dejar inalterado este archivo cuando se apaga el PC. Pero podemos activar el borrado del archivo de intercambio cada vez que lo apaguemos. El único problema es



que aumenta el tiempo de apagado. Sólo lo avisamos.
Entra en regedit mediante Inicio > Ejecutar > regedit
Busca la cadena

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management
```

Selecciona

```
ClearPageFileAtShutdown
```

en la lista de la derecha y con un clic secundario selecciona Cambiar. Cambia el valor a 1 y haz clic en Aceptar. Reinicia el PC.

Secreto numero seis: negativo

Supongamos que olvidamos la contraseña para entrar en Windows XP. Podemos crear un disco de recuperación de la contraseña. El problema es que si olvidamos el disco por ahí, cualquiera podrá cambiar la contraseña de nuestra cuenta.

Vamos a Inicio/Configuración/Panel de Control/Cuentas de usuario y hacemos clic sobre la cuenta de la que queremos crear el disco de recuperación. Un clic sobre Prevenir el



olvido de contraseñas activa el asistente para contraseña olvidada. Insertamos un floppy vacío y seguimos. Para usar el disquete de recuperación en vez de insertar la contraseña, un clic en el signo de interrogación y en la selección del disco de recuperación. Siguiendo el asistente de recuperación de la contraseña se podrá escribir una nueva.



Programando como lo hacía Shakespeare!

El padre del teatro inglés no era programador, pero escribir una comedia de mecanismo perfecto al fin y al cabo es muy parecido a escribir código. En efecto...

¿Sabéis qué han hecho dos estudiantes escandinavos a partir de un estúpido trabajo de análisis para un curso de programación? Han inventado un lenguaje de programación completamente referido a las obras del famoso dramaturgo inglés: el Shakespeare Programming Language, SPL. Hay muchos lenguajes ridículos, pero éste los gana a todos, porque su estructura da al código el aspecto de

FICHA DE IDENTIDAD DEL SPL

Nombre: Shakespeare Programming Language
Nacido en: febrero 2001
Padres: Karl Hasselström y Jon Åslund
Dirección: http://shakespearelang.sourceforge.net/report/shakespeare/
Signos particulares: se convierte directamente en c instrucción por instrucción y combina, dicen irónicamente sus creadores, la expresividad del BASIC con la amigabilidad del lenguaje ensamblador.



una obra teatral de Shakespeare, los personajes entran y salen de escena, dialogan, la obra avanza por actos y todo conserva una coherencia interna admirable, tanto es así que cada gesto, ejem, instrucción en SPL puede convertirse en el más convencional lenguaje C.

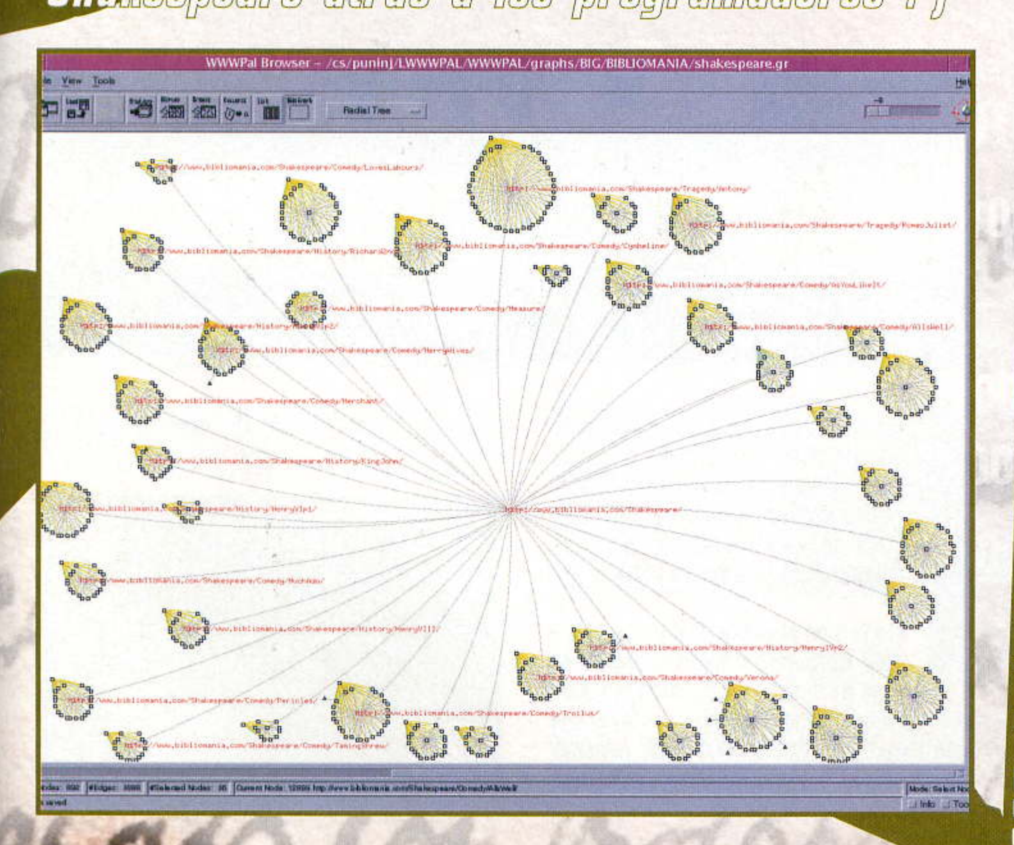
El Shakespeare Programming Language no es particularmente sofisticado; sus estructuras internas se limitan a aritmética de base e instrucciones de salto (goto). Pero aún así puede hacer mucho. La primera parte de un programa de SPL es el título. Puede ser tan largo como quieras. En la práctica el primer párrafo de un programa SPL sirve de título. Luego se introduce a los personajes. Cada uno de ellos en realidad corresponde a una variable, la cual contiene un valor entero. Pero atención: aunque la descripción que sigue a su nombre puede ser fantasiosa, los nombres tienen que ser de verdaderos personajes de Shakespeare, como Romeo, Julieta o Macbeth.

171 BYTE

El Shakespeare Programming Language es fascinante pero produce excesivo código. Para desintoxicar no hay nada mejor que Brainfuck: un lenguaje nacido para tener el compilador más pequeño posible. ¡Hay quien ha conseguido llegar a 171 bytes! Para saber más: http://www.muppetlabs. com/~breadbox/bf.

El programa se divide en actos y los actos se subdividen en escenas, exactamente como en una obra teatral. Pero a efectos de la programación estas escenas son subrutinas y pasar de un acto a otro acto (o escena) tiene el efecto de un goto. Los personajes entran, exactamente como en un escenario, pronuncian sus frases, hacen mutis, etcétera. Leyendo código SPL parece que de un momento a otro puede bajar el telón. Pero a diferencia de una obra teatral, el juego puede seguir durante mucho tiempo, ya que el lenguaje es verdaderamente funcional.

SPL no es el único modo en el que Shakespeare atrae a los programadores :-)



FACTORIZAR O NO FACTORIZAR, ÉSTA ES LA CUESTIÓN

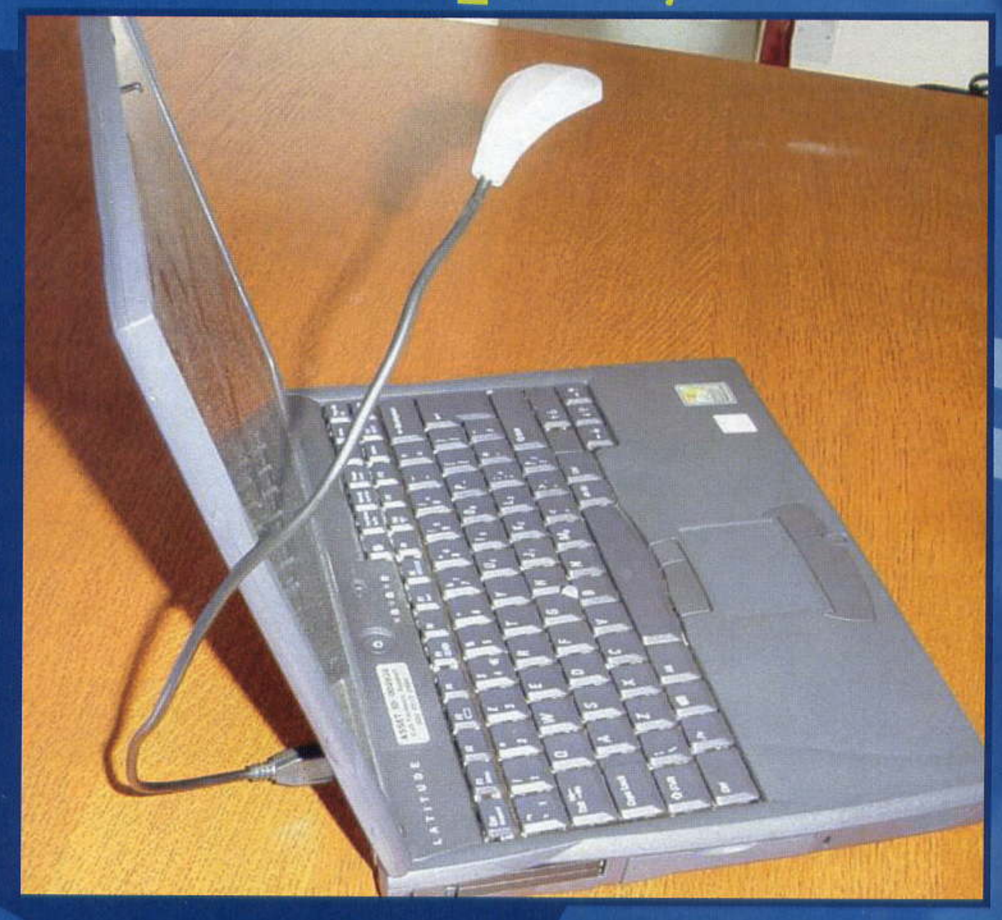
Una de los juegos favoritos de los programadores es intentar adivinar qué hace una función escrita en un lenguaje y probar a repetirla en otro u otros lenguajes. Generalmente se busca la sencillez y la concisión en el código, más que la claridad. Para abreviar, los programadores suelen retarse a redactar rutinas en diversos lenguajes de algoritmos consagrados por el uso. Veamos ahora cómo podría escribirse una función factorial (el factorial de 6 se escribe 6! y significa 1 * 2 * 3 * 4 * 5 * 6 = 720).
El lenguaje Shakespeare Programming Language (http://shakespearelang.sourceforge.net/report/shakespeare/) es capaz de resolver esta cuestión: ¡como puede verse, programar no es tan diferente a escribir teatro!

SHAKESPEARE

```
[enter Hamlet and Romeo]
Hamlet:
You are a sum of an hero and thiself!
Open your hearth!
Romeo:
You lying stupid big smelly coward!
You are a sum of a big knife and thiself!
Speak your mind!
[enter Hamlet and Otello]
Hamlet:
You are a difference from Romeo and a flower!
You are the product of Romeo and thiself!
Open your hearth!
[enter Juliet and Hamlet]
Hamlet:
You are a small red flower!
Romeo:
Am i nicer than you?
Juliet:
If so, let's proceed to Scene IIII
Juliet:
Am i nicer than you?
Romeo:
If so, let's return to Scene I
[enter Romeo and Giulietta]
Giulietta:
Open your earth!
```

HACKING de

A menudo basta con algo de fantasía y algún simple componente para obtener resultados muy satisfactorios. He aquí qué podemos hacer con un puerto USB y un par de leds



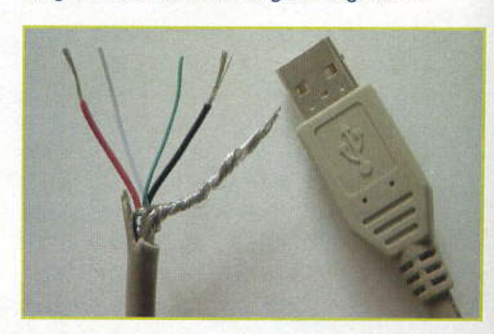
EL MONTAJE

SIGUE EN LA PÁG. 26



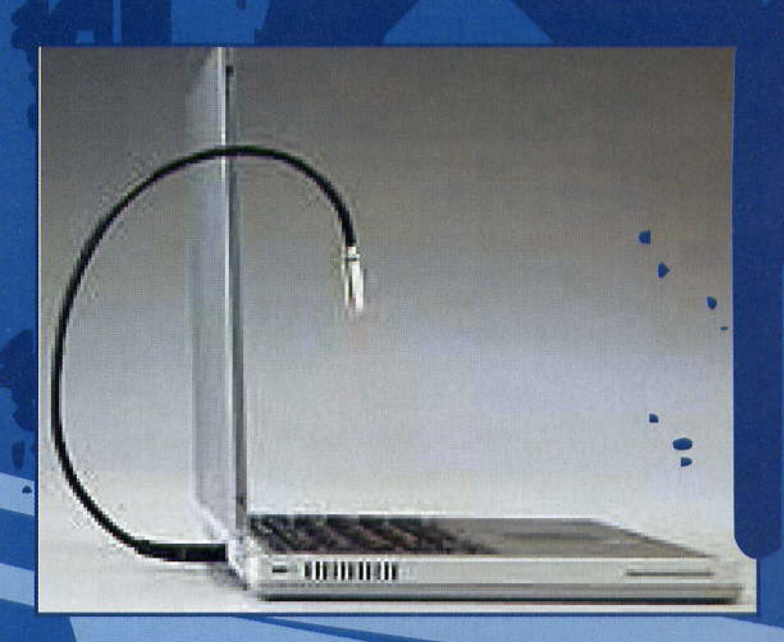
Estos son los componentes necesarios. Del cable USB tenemos que conservar el conector plano que se inserta en el PC. El otro cabo del cable puede tener cualquier tipo de terminación porque no nos interesa: la cortaremos y la desecharemos. Por lo tanto cuidado con equivocarse: se necesita un poco de cable pegado a este conector.

Cortamos el cable USB y con atención quitamos unos dos centímetros de funda. Apartamos la funda metálica y el apantallado metálico y veremos que hay cuatro hilos. Uno blanco y uno verde, generalmente más delgados, y uno rojo y otro negro, que son los de la alimentación y los que nos interesan. En general también son algo más gruesos.



un cable USB

El objetivo es construir una luz brillante y pequeña, para ver de noche, directamente conectable al puerto USB de nuestro PC. Muy útil si tenemos un portátil y nos hallamos en una oscuridad absoluta, o si tenemos que utilizarlo tarde sin molestar a los que están cerca. Conectado a un PC de escritorio y con un cable lo bastante largo, unos tres metros o más, es un útil accesorio para iluminar con precisión y claridad zonas inaccesibles del PC, mientras lo desmontamos, cambiamos tarjetas o switches, etc.



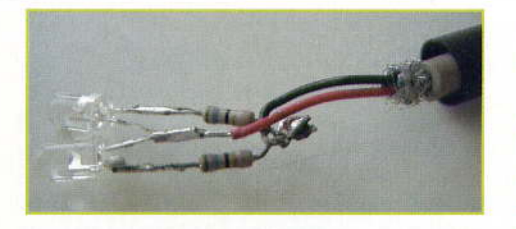
Material necesario

Un cable USB cualquiera, que cortaremos. Por ello tomaremos el más barato posible. Coste aproximado: unos dos euros y se encuentra en las tiendas de informática. Dos leds blancos de alta luminosidad. También pueden ser de colores, para dar a la luz efectos especiales. Pero si queremos una luz que ilumine de veras, pongamos los blancos. Estos componentes son un poco caros: los hemos pagado a 2,75 euros cada uno, pero vale la pena. Los encontraremos en una tienda de componentes electrónicos, o bien en algún sitio web de venta por correo.

Dos resistencias de 56 ohm (también sirven de 47 ohm). Además se puede usar pedazo de vaina termorresistente, útil para sujetar los leds y hacer manejable el conjunto. Evidentemente necesitaremos asimismo un soldador, un poco de estaño, un pelacables o unas tijeras para pelar

Cortamos sin piedad la funda metálica y los hilos blancos y verde. Apartamos y pelamos los hilos rojo, el polo positivo de la alimentación, y negro, el polo negativo. Enhebramos en el cable unos cinco centímetros de cinta termorresistente. Nos servirá para fijar el conjunto, pero no es indispensable: podemos obtener el mismo fin con un trozo de cinta aislante o con otro tipo de cinta (que puedes encontrar en una ferretería).

El principio de la conexión es el siguiente: en serie, se sueldan a los cables de la alimentación la resistencia de 56 ohm y el diodo led.



La resistencia puede montarse en el cable rojo o en el negro, pero con el led hay que respetar la polaridad. El terminal más corto del Led es el cátodo y va señalado también con una muesca en el cuerpo del propio led. El cátodo se conecta al cable negro (-). El terminal más largo es el ánodo y se conecta al cable rojo (+).

Aislamos con mucho cuidado cada fragmento de cable al descubierto con pequeños trozos de cinta aislante. No tienen que tocarse en absoluto: ¡en caso contrario, destruiremos el puerto USB con un cortocircuito!

Estiramos la funda termoaislante hasta cubrir el led, dejando evidentemente descubierta la punta. Con un secador para el pelo, mantenido bien cerca, calentamos la funda, para que for-

los hilos. Es decir, la panoplia de herramientas básicas que todo buen hacker debe tener.

Qué pretendemos

Usamos la tensión presente en la alimentación del puerto USB para encender los dos diodos led montados en paralelo. Evidentemente tenemos que estar atentos a no tomar demasiada corriente para no estropear el puerto y a hacer las cosas con precisión para no crear en ningún caso un cortocircuito que dejaría fuera de servicio el puerto USB de nuestro equipo.

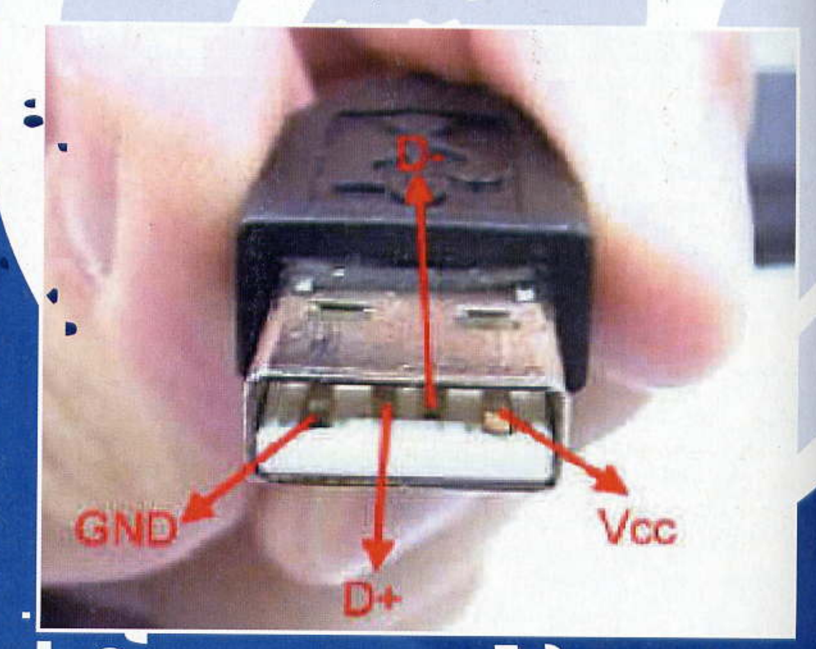


Una luz para puerto USB cuesta alrededor del 15 euros, nosotros hemos gastado menos de 8, pero nos gusta tener la satisfacción de haberlo hecho solos.

USB SIN SECRETOS

En los extremos de la toma USB se encuentra la alimentación, con una tensión de 5 voltios, nada peligrosa, que es posible cargar como máximo con 500 mA. (miliamperios = milésimas de amperio). Si nos pasamos, en el PC aparece un mensaje del controlador que dice que el dispositivo no funciona por exceso de tensión. Por esto se usan los hub USB autoalimentados. Cuando los dispositivos son demasiados, o bien alguno necesita más corriente, es necesario añadir un alimentador externo que proporcione toda la corriente necesaria.

No es el caso de nuestra luz por led. Un led absorbe, en efecto, de 10 a 20 mA y por ello, con un par, llegamos como máximo a una décima parte de la corriente disponible. Nada preocupante.



EL MONTAJE VIENE DE LA PÁG. 25

me un todo con el cable y el cuerpo del led. Así hemos creado una luz manejable y protegida.

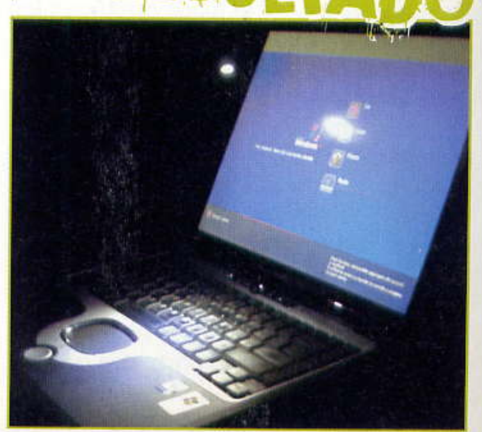
Conectamos el cable al puerto USB y si lo hemos hecho todo con la debida atención funcionara al primer intento: tenemos nuestra propia luz focal y nos sorprenderá hasta qué punto es luminoso este tipo de led.



Incluso en la oscuridad más absoluta tendremos una luz autónoma más que suficiente para iluminar el teclado sin molestar a nadie que pueda estar por los alrededores.

Vale la pena llevar siempre nuestro cable luminoso en la bolsa: ¡como luz de emergencia es absolutamente ideal en mil situaciones! Y siempre puedes contar cómo lo hiciste...







Primos Titánicos



¡Cómo de grande es un gran número y cómo hacerse famoso descubriendo uno!

La matemática es aburrida sólo en la escuela. Luego hay un montón de diversión, especialmente si tenemos un equipo a mano y una mentalidad de hacker. **Por ejemplo, es sabido que los modernos sistemas de cifrado de clave pública** se basan en la generación de números enormes y en la dificultad de recuperar los factores que han generado el número en cuestión.

Por ello encontrar números primos cada vez más grandes es fundamental. Se llaman números primos titánicos ¡y quien los halla puede también adquirir un poco de notoriedad!

Fama (¿y dinero?) con los titánicos

Actualmente el número más titánico de todos es un monstruo: 2^24036583-1. ¡Escrito cifra por cifra requeriría quince números de Hacker Journal! Lo descubrió Josh Findley el pasado 15 de mayo. Josh Findley no es un matemático ni un investigador; es un chico como tantos, pero que se instaló un programa expresamente para efectuar la búsqueda.
Tuvo paciencia, elaborando datos durante más de cinco años. Se requiere también un poco de fortuna: el descubrimiento requirió sólo un par de semanas en un Pentium 4 a 2,4 GHz. Se hará mucho más famoso quien mañana descubra señales de vida inteligente con Seti@Home... pero esta búsqueda es más útil.

Quienes descubren un primo titánico aparecen en la base de datos de la dirección **http://primes.utm.edu/bios/index.php**. ¿Cómo conseguirlo? Descargando el cliente en la dirección http://mersenne.org/freesoft.htm (hay para todos los sistemas: Windows, Linux, Mac OS X) y hacer que funcione todo el tiempo posible.

EL ENIGMA DE LA FACTORIZACIÓN

Si tenemos dos números primos bastante grandes, como 10000000000000357 y 10000000000000709, multiplicarlos es pesado pero no es tan difícil; con un poco de paciencia se puede hacer a mano (¿cuánto da?). Pero con el número 100000000000001066000000000000253113, ¿cómo se averigua qué números hay que multiplicar para obtenerlo? Los programas de cifrado de clave pública se basan en este principio y por ello hallar números primos cada vez más grandes es de tal importancia con fines de cifrado. Si los números no son primos, todo el castillo se cae, y es igualmente difícil saber si un número es primero o no. Un número primo, para quien lo haya olvidado, es divisible sólo por 1 y por sí mismo. El primer número primo es 2. ¿Quién conoce otra propiedad interesante de los números primos?

↑ *Marin Mersenne, 1588-1648. Antes los buscadores de números primos se escondían en monasterios.*

Alguien con suerte puede llegar a conseguir dinero. ¡La Electronic Frontier Foundation ha instituido un premio de cien mil dólares para quien consiga llegar a un número primo con más de diez millones de cifras! Hay también premios superiores, pero esto requerirá tiempo. Todo está explicado en http://www.eff.org/awards/ coop.html.

¿Por qué no ponerse a buscar titánicos? ¡Podría ser útil y seguramente descubriremos algo nuevo!

Bluebugging, la nueva pesadilla de los móviles Bluetooth

Si pensábamos que los dialers eran un problema sólo de los teléfonos fijos, es que no hemos oído hablar aún del Bluebugging.

Imaginemos que podemos controlar un teléfono ajeno, como si estuviera conectado a nuestro portátil, exactamente como hacemos con nuestro teléfono. Resultado: estafa de llamadas telefónicas, invasión masiva de la intimidad y en el futuro también comprar a cargo de otros.

Si ahora le añadimos que todo esto ya es posible, desde hace más de seis meses, entonces estaremos ante uno de los mayores escándalos que ha afrontado jamás la telefonía.

Pero vayamos por orden, y empecemos por el vocabulario. Existen tres tipos distintos de interacción posible con un teléfono Bluetooth (ajeno):

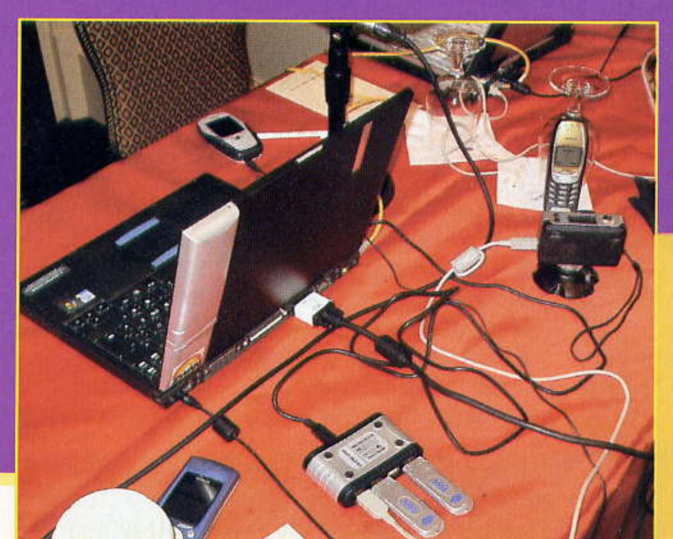
Bluejacking

Esto es el envío de mensajes cuyo contenido va completo en el campo del nombre.

En este modo el mensaje aparece en el teléfono objetivo. En Gran Bretaña se usa normalmente como contacto sexual y muchos chicos y chicas hacen posible voluntariamente esta conexión para vivir la aventura.

Bluesnarfing

Detectado en noviembre de 2003, descubierto por A.L. Digital. Es posible copiar los datos de un teléfono: el registro de llamadas, el código IMEI, la agenda y las fotos; se pueden "actualizar" los datos en el teléfono objetivo.



Bluebugging

Divulgado por Martin Herfurt en marzo de 2004, con ocasión del CeBIT de Hanover. Es

Black Hat: en la mesa todo lo necesario para la demo, pero en realidad basta con un portátil y un dongle bluetooth

posible crear una conexión no autorizada a través de la conexión serie. Acceso completo al set AT del teléfono: se pueden mandar SMS, ejecutar llamadas telefónicas y programar el teléfono.Sus consecuencias quedan claras.

Los dos ponentes en DefCon fueron Adam Laurie <adam@algroup.co.uk>, jefe de seguridad de A.L. Digital, y The Bunker y Martin Herfurt <martin.herfurt@salzburgresearch.at>, responsable de I+D en el Salzburg Research Forschungsgesellschaft mbH. Ambos adivinaron la posibilidad de administrar los teléfonos bluetooth perjudicando al usuario, y pusieron un aviso en el foro de desarrolladores de bluetooth. Durante dos semanas no sucedió nada; entonces lo publicaron todo en el sitio de Slashdot. Resultado: Nokia se puso en contacto con ellos dos días después.
Así, se ha avisado a todos los fabricantes y es interesante ver cuáles ha sido sus respuestas ante la vulnerabilidad descubierta por los autores:
Nokia: contactó inmediatamente a los autores.



Martin Herfurt, a la izquierda, y Adam Laurie durante su intervención en BlackHat.

TDK (desarrolla componentes para móviles): ha publicado un documento que explica que esto no es posible.
SonyEricsson: contactó con los autores y luego publicó un documento donde explica que esto no es posible.
Siemens y Motorola han mandado ejemplares de sus nuevos teléfonos a los autores para verificar su invulnerabilidad.

Si tenéis dudas sobre la posibilidad real de controlar a distancia un teléfono bluetooth, sabed que se realizó una demostración en las conferencias Black Hat y DefCon. Los autores, equipados con un portátil y un dongle bluethoot, empezaron por controlar el teléfono de un "cómplice" suyo sentado en la cuarta fila, el cual se levantó y se alejó por el pasillo, permitiendo a todos los presentes escuchar sus conversaciones. A continuación mandaron SMS a su teléfono desde otro teléfono también de un "cómplice" (para no cometer ningún tipo de delito).

Si con los dialers se llegó tarde, ¿qué queremos hacer con el control de los teléfonos bluetooth? Alrededor de un veinte por ciento de los teléfonos fabricados actualmente es vulnerable, lo cual significa que un malintencionado, por ejemplo cómodamente sentado en una mesa del bar de la estación de Chamartín en Madrid con su portátil con dongle bluetooth, puede localizar diariamente alrededor de doscientos teléfonos vulnerables y hacerles llamar a un número de pago, ¡con un rédito diario de más de 1.000 euros! Entre otras cosas, la conexión bluetooth no deja rastro en los log del teléfono y debido a la imposibilidad de duplicar los teléfonos GSM (aquí también habría MUCHO que hablar) los pobres desafortunados no pueden hacer más que pagar la abultada factura.

Laurie afirma que la mayor parte de las personas olvida apagar el Bluetooth y el modo de descubierta después de haber intercambiado información con un dispositivo (por ejemplo quien usa unos auriculares o un sistema de manos libres en el coche). Alrededor del veinte por ciento de los teléfonos descubiertos en la investigación eran visibles y vulnerable a algún tipo de ataque. En una prueba de dos horas hecha en Londres durante una hora punta, Laurie encontró 336 teléfonos bluetooth, 77 de los cuales eran vulnerables.

EN PELIGRO

Los teléfonos potencialmente expuestos a Bluesnarfing y Bluebugging:

Marca	Modelo	Firmware	Backdoor	Bluesnarfing modalidad Discoverabe	Bluesnarfing modalidad NO Discoverabe	Bluebugging
Ericsson	T68	20R1B 20R2A013 20R2B013 20R2F004 20R5C001	?	Yes	No	No
Sony Ericsson	R520m	20R2G	?	Yes	No	?
Sony Ericsson	T68i	20R1B 20R2A013 20R2B013 20R2F004 20R5C001	?	Yes	?	?
Sony Ericsson	T610	20R1A081 20R1L013 20R3C002 20R4C003 20R4D001	?	Yes	No	?
Sony Ericsson	T610	20R1A081	?	?	?	Yes
Sony Ericsson	Z1010	?	?	Yes	?	?
Sony Ericsson	Z600	20R2C007 20R2F002 20R5B001	?	Yes	?	?
Nokia	6310	04.10 04.20 4.07 4.80 5.22 5.50	?	Yes	Yes	?
Nokia	6310i	4.06 4.07 4.80 5.10 5.22 5.50 5.51	No	Yes	Yes	Yes
Nokia	7650	?	Yes	No (+)	?	No
Nokia	8910	?	?	Yes	Yes	?
Nokia	8910i	?	?	Yes	Yes	?
* Siemens	S55	?	No	No	No	No
* Siemens	SX1	?	No	No	No	No
Motorola	V600 (++)	?	No	No	No	Yes
Motorola	V80 (++)	?	No	No	No	Yes

* Modelos no vulnerables
++ El V600 y el V80 están en modalidad discoverable automáticamente cada 60 segundos cuando se encienden o se selecciona esta función del menú. Motorola ha comunicado que las nuevas versiones del firmware no tendrán este problema.
Origen de los datos: http://www.thebunker.net/release-bluestumbler.htm

CONEXIONES:

http://agentsmith.salzburgresearch.at/
http://www.thebunker.net/release-bluestumbler.htm
Matthew Byng-Maddick <mbm@aldigital.co.uk>

LA MÁQUINA DEL TIEMPO

Recorremos esquemáticamente la historia de la informática moderna desde un punto de vista algo particular: el hacker

1940 – 1970. La era de los mainframes.

1950 J. Presper Eckert Y John W. Mauchly crean el UNIVAC, el primer ordenador que administra la entrada y la información en formato alfanumérico.

1960 La cultura hacker contamina la nacional además de los ordenadores. El centro de la cultura hacker es ahora el MIT y desde aquí la universidad de Carnegie Mellon y Stanford. Los hackers más famosos de estos años son Ed Fredkin, Brian Reid, Jim Gosling, Brian Kernighan, Dennis Ritchie y Richard Stallman.

1969 Nace ARPANET, la primera red de ordenadores que conecta las universidades, la defensa y los laboratorios de investigación privados.

1969 El hacker Ken Thompson crea el sistema operativo UNIX. el hacker Dennis Ritchie crea el lenguaje de programación C.

1971 Un veterano de la guerra del Vietnam, John Draper, descubre que el silbato que viene de obsequio con las cajas del cereal Cap'n Crunch, tiene una frecuencia exacta de 2600 Hz. Draper, ahora conocido como Cap'n Crunch, construye una "blue box" que permite a los phreaks efectuar llamadas telefónicas gratuitas. Al cabo de poco el diario Esquire publica el artículo "Secrets of the Little Blue box" con las instrucciones para construir la Blue box que lleva a Cap'n Crunch a la historia, y poco después, a los federales.

1972 Se funda el InterNetworking Working Group para definir el estándar de la red que se está desarrollando. Al frente del programa está Vinton Cerf, el padre de Internet. Steve Wozniak y Steve Jobs encuentran a Cap'n Crunch y empiezan a vender "blue box" a sus compañeros en la universidad. John Draper es detenido por fraude telefónico. Es su primer arresto y no acaba en prisión.

1973 Robert Metcalfe crea el protocolo Ethernet en el Xerox Palo Alto Research Center (PARC).

1975 Paul Allen y Bill Gates fundan Microsoft (conocida primero como Traf-O-Data) y escriben el BASIC para el ordenador Altair.

1976 Steve Wozniak hace la primera demo del Apple I en el Homebrew Computer Club. John Draper es detenido y condenado por fraude telefónico. Esta vez Captain Crunch va a la cárcel, donde pasa cuatro meses (Lompoc, prisión federal en California) dando cursos de phreaking para ayudar a los compañeros de prisión a llamar a números prohibidos dentro de la cárcel y a interceptar las radios de los vigilantes.



1977 Apple introduce el Apple II y Commodore introduce el orde-

nador PET. John Draper trabaja para Apple con la matrícula 13 y realiza el primer módem (que nunca entró en producción porque era una blue box), que (tras dejar Apple) Captain Crunch utiliza en privado ejecutando decenas de miles de llamadas telefónicas en dos días. ¿Resultado? ¡La habitual visita de los federales e inmediatamente del juez!

1978 Bill Joy y otros desarrollan BSD, una versión del sistema operativo Unix.

1979 Hayes realiza su primer módem y se convierte en el estándar del mercado.

1981 IBM anuncia su Personal Computer.

1982 Se fundan Sun y SGI.

1983 La película Juegos de guerra (War Games) muestra una sombría imagen del hacer de los hackers y los phreakers.

1983 Los servicios secretos obtienen las jurisdicción sobre los casos de fraude con tarjeta de crédito y ordenadores.

1984 Dos chicos, Lex Luthor y Phiber Optik, fundan respectivamente Legion of Doom (LOD) y Masters of Deception (MOD). Otra figura de primer plano es Erik Bloodaxe. Empieza la guerra entre LOD y MOD que concluyó con una gran redada y un día de silencio en los teléfonos americanos. Se funda en Alemania el Chaos Computer Club. En EE.UU. se emite el Comprehensive Crime Control Act. Nace The hacker magazine 2600. El editor es Emmanuel Goldstein (su nombre real es Eric Corley) que toma el nombre de un personaje de 1984 de George Orwell. Orientado al principio a los phreaks, pronto empieza a seguir los problemas de los hackers. Apple anuncia el Macintosh con un anuncio histórico durante la Super Bowl. Borland desarrolla el Turbo Pascal.

1985 Apple da a Microsoft la licencia para algunas funcionalidades de la interfaz gráfica de ventanas. Steve Jobs deja Apple y funda NeXT.

1986 Compaq introduce el primer PC basado en la CPU Intel 80386.

1987 Se crea el CERT para la seguridad de las redes.

1988 El primer gusano: The Morris Worm. Robert t. Morris, Jr. (RTM), estudiante de la universidad de Cornell, hijo de uno de los científicos de la National Security Agency, escribe y ejecuta el código de un gusano que se replica en ARPAnet para verificar los efectos en sistemas UNIX. Fuera de control, el gusano infecta 6.000 máquinas bloqueando la red gubernativa y universitaria. Morris es cazado en Cornell y condenado a tres años de vigilancia y una multa de 10.000 dólares. Kevin Mitnick controla el mail de la MCI y Digital Equipment. ¿Resultado? Kevin Mitnick es condenado a un año de cárcel.

1990 Tim Berners-Lee inventa el World Wide Web creando HTTP y HTML. El fin de un mito: Peter Norton vende su empresa y su imagen a Symantec.

1991 Linus Torvals presenta su proyecto: Linux. Es también el año del virus Michelangelo debía hacer estragos en los ordenadores el 6 de marzo de 1992 en ocasión del cumpleaños del artista. Pero no sucede nada.

1992 Microsoft lanza Windows 3.1.

1993 El año del primer Def Con, la conferencia de los hackers en Las Vegas. El proyecto original es una fiesta de despedida al BBS y la bienvenida a Internet pero se transforma en un acontecimiento anual.

1994 Mark Andreessen y James Clark fundan Netscape.

1995 En febrero el FBI detiene a Kevin Mitnick. La acusación es haber robado 20.000 números de tarjetas de crédito y causar unos daños de 120 millones de dólares al apoderarse del código fuente de un móvil de Motorola y parte del código de Solaris. Permanece en la cárcel cuatro años sin ser procesado.

1997 Microsoft Internet Explorer adelanta a Netscape Communicator en el mercado de los navegadores.

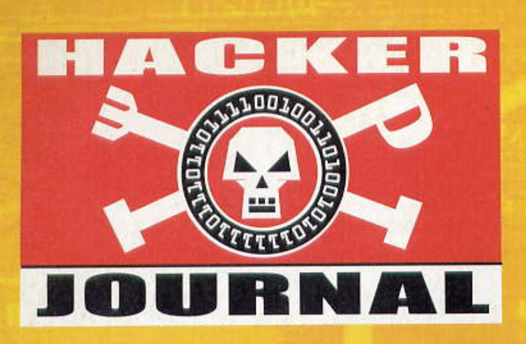
1998 El grupo Cult of the Dead Cow inventa y lanza el troyano Back Orifice en ocasión de Def Con. Linux se convierte en el segundo S.O. en crecimiento.

1999 Kevin Mitnick, detenido desde 1995 firma un acuerdo para su liberación. Nace el virus Melissa, el más difundido de todos.

2000 Kevin Mitnick sale de prisión.

2001 Microsoft es objeto de un DOS a través del DNS. El lugar sigue funcionando pero los usuarios no pueden acceder a él durante casi dos días.

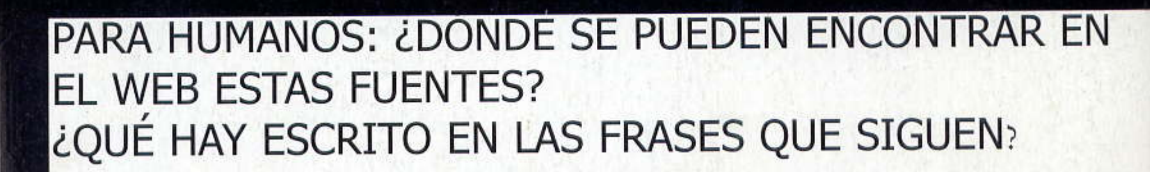




EL PRÓXIMO NÚMERO EN EL QUIOSCO ¡el 1 de marzo de 2005!

CYBERENIGMA

¡Felices runas!



PARA HUMANOS: ¿DONDE SE PUEDEN ENCONTRAR EN EL WEB ESTAS FUENTES?
¿QUÉ HAY ESCRITO EN LAS FRASES QUE SIGUEN?

Enviad las respuestas a:

redaccion@hacker-journal.com